PCT/JP00/05482

16.08.00

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

RECD 04 SEP 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 ８月２０日

09/807702

出願番号
Application Number: 平成１１年特許願第２３４３６８号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年 ６月２９日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０４９９７６

【書類名】　特許願
【整理番号】　9900283403
【提出日】　平成11年 8月20日
【あて先】　特許庁長官　殿
【国際特許分類】　G11B　7/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　浅野　智之
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　大澤　義知
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　加藤　元樹
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100067736
【弁理士】
【氏名又は名称】　小池　晃
【選任した代理人】
【識別番号】　100086335
【弁理士】
【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録／再生システム、情報記録装置及び情報再生装置

【特許請求の範囲】

【請求項１】　暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、

上記暗号化コンテンツ情報からコンテンツ情報を暗号鍵により復号するコンテンツ情報復号手段と、

上記暗号鍵を暗号化する暗号鍵暗号化手段と、

上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号鍵記録手段と、

上記コンテンツ情報復号手段により復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、

上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備える情報記録装置と、

上記情報記録装置により暗号化コンテンツ情報と暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、

上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、

上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、

上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、

上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を復号する暗号鍵復号手段とを備える情報再生装置と

からなることを特徴とする情報記録／再生システム。

【請求項２】　上記情報記録装置は、通信手段を用いて他の装置から伝送されてきた暗号化コンテンツ情報と該コンテンツ情報を暗号化するのに用いられた暗号鍵を受信する受信手段を備え、上記受信手段により受信した暗号鍵を上記暗号

鍵暗号化手段で暗号化するとともに、上記受信手段により受信した暗号鍵を用いて上記受信手段により受信した暗号化コンテンツ情報からコンテンツ情報を上記コンテンツ情報復号手段により復号して、上記管理情報生成手段により管理情報を生成することを特徴とする請求項１記載の情報記録／再生システム。

【請求項３】　上記暗号化コンテンツ情報は、映像情報であることを特徴とする請求項１記載の情報記録／再生システム。

【請求項４】　上記暗号化コンテンツ情報は、音楽情報であることを特徴とする請求項１記載の情報記録／再生システム。

【請求項５】　暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、

上記暗号化コンテンツ情報を復号するコンテンツ情報復号手段と、

上記コンテンツ情報復号手段により暗号化コンテンツ情報から復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、

上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段と

を備えることを特徴とする情報記録装置。

【請求項６】　通信手段を用いて他の装置から伝送されてきた暗号化コンテンツ情報と該コンテンツ情報を暗号化するのに用いられた暗号鍵を受信する受信手段と、

上記受信手段により受信した暗号鍵を暗号化する暗号鍵暗号化手段と、

上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号化暗号鍵記録手段と

をさらに備え、

上記コンテンツ情報復号手段は、上記受信手段により受信した暗号鍵を用いて、上記受信手段により受信した暗号化コンテンツ情報からコンテンツ情報を復号することを特徴とする請求項５記載の情報記録装置。

【請求項７】　記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記暗号鍵暗号化手段により上記暗号鍵を暗号化するために用いる第１の暗号鍵を決定する第１の暗号鍵生成手段と

をさらに備えることを特徴とする請求項６記載の情報記録装置。

【請求項８】　上記暗号鍵暗号化手段により上記暗号鍵を暗号化するために用いる第１の暗号鍵を決定する第１の暗号鍵生成手段と、

上記記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記第１の暗号鍵を暗号化するために用いる第２の暗号鍵を決定する第２の暗号鍵生成手段と

をさらに備えることを特徴とする請求項６記載の情報記録装置。

【請求項９】　記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体に暗号化して格納されている第１の暗号鍵を読み出す暗号鍵読出手段と、

上記暗号鍵読出手段により読み出される暗号化された第１の暗号鍵を復号するための第２の暗号鍵を上記記録媒体識別情報読出手段により読み出された記録媒体識別情報に基づいて決定する第２の暗号鍵生成手段と、

上記第２の暗号鍵生成手段で生成された第２の暗号鍵を用いて暗号化された第１の暗号鍵を復号する第１の暗号鍵復号手段と

をさらに備え、

上記暗号鍵暗号化手段は、上記受信手段により受信した暗号鍵を上記第１の暗号鍵復号手段により復号された第１の暗号鍵を用いて暗号化することを特徴とする請求項６記載の情報記録装置。

【請求項１０】　暗号化コンテンツ情報と該暗号化コンテンツ情報からコンテンツ情報を復号するための暗号鍵を暗号化した暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、

上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、

上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手

段と、

上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、

上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を第１の暗号鍵により復号する暗号鍵復号手段とを備える

ことを特徴する情報再生装置。

【請求項１１】　記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記暗号鍵復号手段により上記暗号鍵を復号するために用いる第１の暗号鍵を決定する第１の鍵生成手段とをさらに備える

ことを特徴とする請求項１０記載の情報再生装置。

【請求項１２】　上記暗号鍵復号手段により上記暗号鍵を復号するために用いる第１の暗号鍵を決定する第１の鍵生成手段と、

上記記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記第１の暗号鍵を暗号化するために用いる第２の暗号鍵を決定する第２の鍵生成手段とをさらに備える

ことを特徴とする請求項１０記載の情報再生装置。

【請求項１３】　記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体に暗号化して格納されている第１の暗号鍵を読み出す暗号鍵読出手段と、

上記暗号鍵読出手段により読み出される暗号化された第１の暗号鍵を復号するための第２の暗号鍵を上記記録媒体識別情報読出手段により読み出された記録媒体識別情報に基づいて決定する第２の鍵生成手段と、

上記第２の鍵生成手段で生成された第２の暗号鍵を用いて暗号化された第１の暗号鍵を復号する第１の暗号鍵復号手段とをさらに備える

ことを特徴とする請求項１０記載の情報再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録装置及び情報再生装置に関する。

【０００２】

【従来の技術】

近年、情報をデジタル的に記録する記録機器及び記録媒体が普及しつつある。これらの記録機器及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データの質を維持しながら何度もデータをコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【０００３】

このような著作権保護のためのシステムとして、例えば、ミニディスク（MD）（商標）システムにおいては、ＳＣＭＳ(Serial Copy Management System) と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、ＳＣＭＳを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【０００４】

このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００５】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、ＤＶＤシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記のミニディスクシステムが採用している方式では、ＳＣＭＳがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【０００７】

また、上記のＤＶＤシステムが採用している方式は、ＲＯＭメディアに対しては有効であるが、ユーザがデータを記録可能なＲＡＭメディアにおいては有効ではない。ＲＡＭメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【０００８】

そこで、本件出願人が先に出願した特願平１０－２５３１０号の特許出願においては、個々の記録媒体を識別するための情報（以下、媒体識別情報とよぶ）を記録媒体に持たせ、この情報はライセンスを受けた機器しかアクセスできないようにしている。すなわち、記録媒体上のデータは媒体識別情報と、ライセンスを受けることによって得られる秘密に基づく鍵によって暗号化し、ライセンスを受

けていない機器はデータを読み出しても意味のないものとしている。さらに機器にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。ライセンスを得ていない機器は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体ごとに個別の値になっているため、ライセンスを受けていない機器がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない機器でもライセンスを受けた機器でも正しく情報が読み出せないようにしている。

【０００９】

ところで、上記特許出願に係る記録機器では、他の機器とデータの送受信を行える例えばＩＥＥＥ１３９４などのインタフェースを備えており、他の機器から伝送されたコンテンツデータを記録媒体に記録する場合が考えられる。

【００１０】

この場合、コンテンツデータは、インタフェース上を、例えば、ソニー、松下、日立、東芝、インテルの５社によって開発された、Digital Transmission Content Protection 規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記した White Paper を、ライセンス組織である Digital Transmission Licensing Administrator (DTLA) のウェブページであるhttp://www.dtcp.com から誰でも取得することが可能である） を用いて暗号化されて伝送されることが考えられる。この際、コンテンツデータはコンテンツキー Ｋｃを用いて暗号化されて伝送され、さらに コンテンツキー Ｋｃ自身も暗号化されるなど、安全な方法で上記記録機器に伝送される。

【００１１】

記録機器が伝送されたコンテンツデータを安全に、すなわち不正コピーを許さないように、記録媒体に記録する最も簡単な方法は、暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録することである。

【００１２】

このようにすれば、記録機器は記録時に、大容量のコンテンツデータの処理が

ただ受信して記録するだけでよくなり、簡便に行える。

【００１３】

しかしながら、上記の方式においては、コンテンツデータは暗号化されたまま記録機器に伝送されて媒体に記録されているため、再生時に不便である。

【００１４】

すなわち、本来であれば、ＡＶコンテンツを再生する際には、特に、早送り又は巻き戻ししながらの再生など、いわゆるトリックプレイを行うためには、コンテンツデータのフォーマットと構造を認識して、それに対応して記録媒体のどのデータを読み出すかを決定するなどの制御を行う必要がある。

【００１５】

ところが、上記の方式においては、記録媒体からコンテンツデータを読み出して復号してみない限り、媒体のどこにどのデータが記録されているかを制御部が認識することができず、きめ細かなトリックプレイが行えないという問題点がある。

【００１６】

そこで、本発明の目的は、暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録し、しかも、きめ細かなトリックプレイを行うことができるようにした情報記録／再生システム、情報記録装置及び情報再生装置を提供することにある。

【００１７】

【課題を解決するための手段】

本発明では、記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータを復号して、再生時に必要な管理情報を集めたマップファイルを作成し、これをコンテンツデータとともに記録するようにすることで上記の課題を解決する。

【００１８】

すなわち、本発明に係る情報記録／再生システムは、暗号化コンテンツ情報を

暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、上記暗号化コンテンツ情報からコンテンツ情報を暗号鍵により復号するコンテンツ情報復号手段と、上記暗号鍵を暗号化する暗号鍵暗号化手段と、上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号鍵記録手段と、上記コンテンツ情報復号手段により復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備える情報記録装置と、上記情報記録装置により暗号化コンテンツ情報と暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を復号する暗号鍵復号手段とを備える情報再生装置とからなることを特徴とする。

【００１９】

また、本発明に係る情報記録装置は、暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、上記暗号化コンテンツ情報を復号するコンテンツ情報復号手段と、上記コンテンツ情報復号手段により暗号化コンテンツ情報から復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備えることを特徴とする。

【００２０】

さらに、本発明に係る情報再生装置は、暗号化コンテンツ情報と該暗号化コンテンツ情報からコンテンツ情報を復号するための暗号鍵を暗号化した暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、上記記

録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を第１の暗号鍵により復号する暗号鍵復号手段とを備えることを特徴する。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【００２２】

本発明は、例えば図１に示すような構成の光ディスク記録／再生装置１０に適用される。

【００２３】

この図１に示した光ディスク記録／再生装置１０は、光ディスク１１を回転駆動するスピンドルモータ１２、上記光ディスク１１の情報記録面を光学的に走査する記録／再生ヘッド１３、上記記録／再生ヘッド１３により得られる再生信号に基づいて上記スピンドルモータ１２を制御するサーボ回路１４、上記記録／再生ヘッド１３により上記光ディスク１１を介してデータの記録／再生を行う記録／再生部１５、入力操作部１６から入力される設定情報に基づいて上記サーボ回路１４や記録／再生部１５を制御する制御回路１７等を備える。

【００２４】

上記スピンドルモータ１２は、サーボ回路１４による制御に基づいて、上記光ディスク１１を例えば線速度一定の状態で回転駆動させる。

【００２５】

上記記録／再生ヘッド１３は、上記スピンドルモータ１２により回転駆動される光ディスク１１の情報記録面を光学的に走査して、データの記録／再生を行う。

【００２６】

上記サーボ回路１４は、上記光ディスク１１を所定の速度で（例えば線速度一定で）回転させるようにスピンドルモータ１２を駆動するとともに、記録／再生

ヘッド１３のトラッキング制御、フォーカシング制御やスレッディング制御を行う。

【００２７】

上記記録／再生部１５は、上記制御回路１７により制御されて動作する暗号化処理部４と復号処理部５を有する。暗号化処理部４は、記録モード時に、外部から供給される記録信号を暗号化し、暗号化した記録信号を上記記録／再生ヘッド１３に供給して、光ディスク１１に記録させる。また、復号処理部５は、再生モード時に上記記録／再生ヘッド１３により光ディスク１１から再生された再生データを復号し、外部に再生信号として出力する。

【００２８】

上記入力操作部１６は、図示しない操作ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。

【００２９】

上記制御回路１７は、図示しないメモリに記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【００３０】

この実施の形態において、光ディスク１１は、図２に示すように、リードインエリアＡＲreadinとデータエリアＡＲdataからなる。

【００３１】

そして、光ディスク１１のリードインエリアＡＲreadinには、記録媒体の識別情報（以下、DiscIDと称する）を記録システム共通の予め定められた方法で変換した（これを便宜上、本出願においては、”システム共通秘密で暗号化した”と呼ぶことにする）ＥDiscIDと、ディスクキーＫｄをイフェクティブマスタキーＫｅｍで暗号化した暗号化ディスクキーＥＫｄが記録されている。

【００３２】

なお、媒体識別情報DiscIDを変換する方法すなわちシステム共通秘密は、著作権者から適正なライセンスを受ける際、後述するマスタキーＫｍとともに、ライセンスを受けた者に与えられる。

【００３３】

例えば、媒体識別情報DiscIDを変換する方法のひとつとして、所定のＭ系列符号に基づいて光ディスクの情報を表すピットのエッジの時間ずれとする方法がある。この場合、DiscIDをこのような方法で変換するということと、Ｍ系列符号がシステム共通秘密となり、媒体識別情報DiscIDはその両方がないと読み取る（復号する）ことができなくなる。

【００３４】

このようなＭ系列符号に基づく暗号化に関する技術は、特願平９－２８８９６０号として本出願人が先に提案している。なお、この所定のシステム共通秘密は、著作権者から適正なライセンスを受ける際、後述するマスタキーＫｍとともに、ライセンスを受けた者に与えられる。

【００３５】

イフェクティブマスタキーＫｅｍは、式（１）に従い、マスタキーＫｍとDiscIDの結合にhash関数を適用して計算される。

【００３６】

Ｋｅｍ＝ｈａｓｈ（Ｋｍ＋DiscID）　　（１）

ここで、マスタキーＫｍは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。また、例えば、ＡとＢの結合とは、それぞれが３２ビットであるとき、Ａの後方にＢを結合して、６４ビットのデータとすることを意味する。

【００３７】

また、光ディスク１１のデータエリアＡＲdataを構成する各セクタＳｉ（ｉ＝１，２，・・・）は、ヘッダＨＤ及びメインデータ部ＭＤで構成され、ヘッダＨＤには、コンテンツキーＫｃをディスクキーＫｄで暗号化した暗号化コンテンツキーＥＫｃが格納されている（ここでＳｉのｉは、セクタの番号を示すが、特に個々のセクタを区別する必要がない場合は、ｉを省略する）。メインデータ部ＭＤには、コンテンツデータをコンテンツキーＫｃで暗号化した、すなわち伝送された記録機器で受信された暗号化コンテンツデータが格納されている。

【００３８】

上記光ディスク記録／再生装置１０における暗号化処理部４は、その具体的な構成を図３に示すように、DiscID暗号化復号回路４１、Ｋｅｍ発生モジュール４２、乱数発生回路４３、Ｋｄ暗号化復号回路４４、Ｋｃ暗号化回路４５やコンテンツデータ復号回路４６、マップファイル生成回路４７等からなる。

【００３９】

上記DiscID暗号化復号回路４１は、上記記録／再生ヘッド１３により光ディスク１１のリードインエリアＡＲreadinから読み出されたＥDiscIDをDiscID暗号化復号回路４１に含まれるシステム共通秘密に基づいて復号することにより、媒体識別情報DiscIDを生成する。また、このDiscID暗号化復号回路４１は、乱数発生回路４３により発生された乱数を媒体識別情報DiscIDとして受け取り、システム共通秘密に基づいて、上述したように暗号化して、ＥDiscIDを生成する。このDiscID 暗号化復号回路４１により上記乱数から生成されたＥDiscIDは、上記記録／再生ヘッド１３を介して光ディスク１１のリードインエリアＡＲreadinに記録される。

【００４０】

上記Ｋｅｍ発生モジュール４２は、マスタキーＫｍを記憶するＫｍメモリ４２Ａと、上記マスターキーＫｍと媒体識別情報DiscIDとからイフェクティブマスタキーＫｅｍを生成するハッシュ関数回路４２Ｂからなる。上記ハッシュ関数回路４２Ｂは、上述の（１）式に従って、マスタキーＫｍとＤｉｓｃＩＤの結合を生成し、これにｈａｓｈ関数を適用してイフェクティブマスタキーＫｅｍを生成する。そして、上記ハッシュ関数回路４１Ｂは、生成したイフェクティブマスターキーＫｅｍをＫｄ暗号化復号回路４４に供給する。

【００４１】

上記Ｋｄ暗号化復号回路４４は、上記記録／再生ヘッド１３により光ディスク１１のリードインエリアＡＲreadinから読み出された暗号化ディスクキーＥＫｄをイフェクティブマスタキーＫｅｍで復号して、ディスクキーＫｄを生成する。また、このＫｄ暗号化復号回路４４は、乱数発生回路４３により発生された乱数をディスクキーＫｄとして受け取り、イフェクティブマスタキーＫｅｍで暗号化

して暗号化ディスクキーＥＫｄを生成する。このＫｄ暗号化復号回路４４により生成された暗号化ディスクキーＥＫｄは、上記記録／再生ヘッド１３を介して光ディスク１１のリードインエリアＡＲreadinに記録される。

【００４２】

上記Ｋｃ暗号化回路４５は、他の機器とのインタフェース部から受け取ったコンテンツキーＫｃをディスクキーＫｄで暗号化して暗号化コンテンツキーＥＫｃを生成する。このＫｃ暗号化回路４５により生成された暗号化コンテンツキーＥＫｃは、上記記録／再生ヘッド１３を介して光ディスク１１のデータエリアＡＲdataに記録される。

【００４３】

インタフェース部からわたされた暗号化されたコンテンツデータはそのまま上記記録／再生ヘッド１３を介して光ディスク１１のデータエリアＡＲdataに記録される。

【００４４】

上記コンテンツデータ復号回路４６は、コンテンツキーＫｃでコンテンツデータを復号し、マップファイル生成回路４７に与える。

【００４５】

上記マップファイル生成回路４７は、復号されたコンテンツデータから、再生時に必要な情報を集めたマップファイルを生成する。このマップファイル生成回路４７により生成されたマップファイルは、上記記録／再生ヘッド１３を介して光ディスク１１のデータエリアＡＲdataに記録される。

【００４６】

ここで、コンテンツデータがＭＰＥＧ２トランスポートストリームである場合について、上記マップファイル生成回路４７の具体的な構成例を示す図４のブロック図を参照して説明する。

【００４７】

このマップファイル生成回路４７において、ＡＶプログラムが多重化されているＭＰＥＧ２トランスポートストリームが端子４７１を介して入力されるＰＩＤフィルター４７２、上記ＰＩＤフィルター４７２により取り出されたＰＩＤのト

ランスポートパケットがスイッチ４７３を介して供給されるＰＡＴ／ＰＭＴ解析部４７４及びストリーム解析部４７５と、上記ＰＩＤフィルター４７２により取り出されたＰＩＤのトランスポートパケット供給されるカウンタ４７６と、上記ＰＡＴ／ＰＭＴ解析部４７４及びストリーム解析部４７５による各解析結果が与えられるマップデータ作成部４７７と、上記マップデータ作成部４７７に接続されたファイルシステム４７８等から成る。

【００４８】

上記端子４７１を介して入力されるトランスポートストリームは、トランスポートパケットが連続したストリームであり、トランスポートパケットは、ＭＰＥＧ２ビデオストリームやＭＰＥＧ１オーディオストリームがパケット化されたものである。

【００４９】

ＰＩＤフィルター４７２は、入力されたトランスポートストリームの中から指定されたＰＩＤのトランスポートパケットを取り出す。ＰＩＤは、トランスポートパケットのヘッダの固定位置にある１３ビット長の符号であり、そのトランスポートパケットのペイロード（トランスポートパケットのヘッダに続くデータ部分）にストアーされているデータのタイプを表す。

【００５０】

はじめにＰＩＤフィルター４７２は、ＰＩＤ＝０ｘ０００００であるＰＡＴ(Program Association Table)のトランスポートパケットを取り出す。ＰＩＤフィルター４７２から出力されるＰＡＴのトランスポートパケットは、スイッチ４７３からＰＡＴ／ＰＭＴ解析部４７４へ入力される。

【００５１】

ここで、ＰＡＴ／ＰＭＴ解析部４７４の動作について、図５に示すフローチャートを用いて説明する。

【００５２】

ステップＳ１で、ＰＡＴ／ＰＭＴ解析部４７４は、ＰＡＴのトランスポートパケットを受信する。ＰＡＴには、トランスポートストリームに多重化されているＡＶプログラムのＰＭＴ(Program Map Table)のトランスポートパケットのＰＩ

Ｄが書かれている。

【００５３】

ステップＳ２で、ＰＡＴ／ＰＭＴ解析部４７４はＡＶプログラムのＰＭＴのＰＩＤをＰＩＤフィルターにセットする。ＰＩＤフィルター４７２は、ＰＭＴのＰＩＤをもつトランスポートパケットを取り出すと、それをＰＡＴ／ＰＭＴ解析部４７４へ入力する。

【００５４】

ステップＳ３で、ＰＡＴ／ＰＭＴ解析部４７４は、ＰＭＴのトランスポートパケットを受信する。ＰＭＴには、ＡＶプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポートパケットのＰＩＤが書かれている。ＰＡＴ／ＰＭＴ解析部４７４は、ＡＶプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポートパケットのＰＩＤを取得する。

【００５５】

ステップＳ４で、ＰＡＴ／ＰＭＴ解析部４７４は、ＡＶプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポートパケットのＰＩＤをＰＩＤフィルターとストリーム解析部４７５にセットして、動作を終了する。

【００５６】

そして、上記ＰＡＴ／ＰＭＴ解析部４７４は、マップデータ作成部４７７へ次のパラメータを与える。

【００５７】

（Ａ）　ＡＶプログラムのＰＭＴのトランスポートパケットのＰＩＤ

（Ｂ）　ＡＶプログラムを構成するビデオのトランスポートパケットのＰＩＤ及びビデオのｓｔｒｅａｍ＿ｔｙｐｅ

（Ｃ）　ＡＶプログラムを構成するオーディオのトランスポートパケットのＰＩＤ及びオーディオのｓｔｒｅａｍ＿ｔｙｐｅ

（Ｄ）　ＡＶプログラムのＰＣＲ＿ＰＩＤ

ここで、ｓｔｒｅａｍ＿ｔｙｐｅとは、ＰＭＴに書いてある内容であり、ビデ

オの場合、ＭＰＥＧ２／ＭＰＥＧ１などのストリームタイプを表し、またオーディオの場合、ＭＰＥＧ１／ＡＣ－３などのストリームタイプを表す。

【００５８】

そして、ＰＩＤフィルター４７２は、ＰＡＴ／ＰＭＴ解析部４７４から指定されたビデオのトランスポートパケットとオーディオのトランスポートパケットを入力トランスポートストリームの中から取り出すと、それをスイッチ４７３を介してストリーム解析部４７５へ入力する。ビデオのトランスポートパケットとオーディオのトランスポートパケット以外のトランスポートパケット（サービスインフォメーションのパケットなど）は、ストリーム解析部４７５へ入力されない。

【００５９】

ＰＩＤフィルター４７２から出力されるトランスポートパケットは、カウンター４７６へ入力される。カウンター４７５は、記録するトランスポートストリームの先頭パケットから現在のパケットまでのバイト数を計算し、その値をストリーム解析部４７５に与える。

【００６０】

ストリーム解析部４７５は、ＡＶプログラム中のランダムアクセス再生できるポイントを抽出する。ビデオデータのランダムアクセスポイントのトランスポートパケットは、ＭＰＥＧビデオのシーケンスヘッダとそれに続くＩピクチャデータをペイロードに持つパケットである。ビデオデータのランダムアクセスポイントリストの概念図を図６に示す。ランダムアクセスポイントは、ランダムアクセスするトランスポートパケットのタイムスタンプとデータ読み出し開始のアドレスを表す。ここで、タイムスタンプは、ランダムアクセスポイントのトランスポートパケットの記録器への入力時刻、又は、ランダムアクセスポイントのＩピクチャのＰＴＳ(Presentation Time Stamp) に基づいて計算される。ＰＴＳは、ＭＰＥＧ２システムズ規格のＰＥＳパケットのヘッダに付加されている情報である。なお、この図６ではトランスポートストリームファイルをトランスポートパケットが連続して記録されている形で示しているが、トランスポートパケット毎に、そのパケットの記録器への入力時刻を示すタイムスタンプを付加して記録して

も良い。このタイムスタンプは、例えば、ＤＶフォーマットで規定されているところのトランスポートパケットに付加される４バイト長のＴＳＰ＿ｅｘｔｒａ＿ｈｅａｄｅｒと同様なものである。

【００６１】

ビデオデータ及びオーディオデータのランダムアクセスポイント情報は、マップデータ作成部４７７に与えられる。マップデータ作成部４７７は、ランダムアクセスポイント情報をテーブル化する。

【００６２】

マップデータ作成部４７７は、マップデータテーブルをファイルシステム４７８に与える。

【００６３】

ファイルシステム４７８は、マップデータテーブルをファイル化して出力する。

【００６４】

図７は、トランスポートストリームとマップファイルの説明図である。マップファイルは、次のデータを持つ。

【００６５】

１．　ＡＶプログラムのＰＭＴのトランスポートパケットのＰＩＤ

２．　ＡＶプログラムを構成するビデオのトランスポートパケットのＰＩＤ及びビデオのｓｔｒｅａｍ＿ｔｙｐｅ

３．　ＡＶプログラムを構成するオーディオのトランスポートパケットのＰＩＤ及びオーディオのｓｔｒｅａｍ＿ｔｙｐｅ

４．　ＡＶプログラムのＰＣＲ＿ＰＩＤ

５．　ＡＶビデオのランダムアクセスポイントのリスト

６．　ＡＶオーディオのランダムアクセスポイントのリスト

上記光ディスク記録／再生装置１０における復号処理部５は、その具体的な構成を図８に示すように、ＥDiscID復号回路５１、Ｋｅｍ発生モジュール５２、Ｋｄ復号回路５４、Ｋｃ復号回路５５等からなる。

【００６６】

ＥDiscID復号回路５１は、上記記録／再生ヘッド１３により光ディスク１１のリードインエリアＡＲreadinから読み出されたＥDiscIDを自身が持つシステム共通秘密に基づいて復号して、媒体識別情報DiscIDを生成する。このＥDiscID復号回路５１は、生成した媒体識別情報DiscIDをＫｅｍ発生モジュール５２に与える。

【００６７】

Ｋｅｍ発生モジュール５２は、マスタキーＫｍを記憶するＫｍメモリ５２Ａと、上記マスターキーＫｍと媒体識別情報DiscIDとからイフェクティブマスタキーＫｅｍを生成するハッシュ関数回路５２Ｂからなる。上記ハッシュ関数回路５２Ｂは、上述の（１）式に従って、マスタキーＫｍとＤｉｓｃＩＤの結合を生成し、これにｈａｓｈ関数を適用してイフェクティブマスタキーＫｅｍを生成する。そして、上記ハッシュ関数回路４１Ｂは、生成したイフェクティブマスターキーＫｅｍをＫｄ復号回路５４に供給する。このＫｅｍ発生モジュール５２は、上述のＫｅｍ発生モジュール４２と同一の構成とし、両者を兼用するようにしてもよい。

【００６８】

ＥＫｄ復号回路５４は、上記記録／再生ヘッド１３により光ディスク１１のリードインエリアＡＲreadinから読み出された暗号化ディスクキーＥＫｄをイフェクティブマスタキーＫｅｍで復号して、ディスクキーＫｄを算出する。

【００６９】

ＥＫｃ復号回路５５は、光ディスク１１のデータエリアＡＲdataから上記記録／再生ヘッド１３により読み出される各セクタＳｉのヘッダに記録されている暗号化コンテンツキーＥＫｃをディスクキーＫｄで復号して、コンテンツキーＫｃを算出する。

【００７０】

なお、図８に示した復号処理部５では、暗号化されたまま読み出されたコンテンツデータと復号したコンテンツキーＫｃとを、データインタフェース部に渡すようになっている。これは例えば、このコンテンツを他の機器に伝送するような

場合に用いられる。

【００７１】

これに対し、図９に示す復号処理部５は、光ディスク１１のデータエリアＡＲdataから上記記録／再生ヘッド１３により読み出された暗号化コンテンツデータをＥＫｃ復号回路５５で復号したコンテンツキーＫｃにより復号して平文コンテンツデータを生成するコンテンツ復号回路５６を備えている。

【００７２】

この図９に示す復号処理部５は、例えば、この再生機器においてこの後コンテンツデータに施されているＭＰＥＧなどの符号が復号され、Ｄ／Ａコンバータを通して画像として出力される場合に用いられる。

【００７３】

なお、この再生処理を行う際に、記録時に作成されたマップファイルに含まれる情報を用いて、制御回路１７により光ディスク１１からのコンテンツデータの読み出しを制御する。

【００７４】

図１０は、マップファイルに含まれる情報を用いてコンテンツデータの読み出しを制御するコンテンツデータ再生装置のブロック図を示す。ここでは、上述の図４で説明したマップファイル生成回路４７で作成したマップファイルの情報を用いて、そのマップファイルに対応するトランスポートストリームファイルの読み出しを制御するトランスポートストリーム再生装置を説明する。

【００７５】

記録媒体６０には、トランスポートストリームファイルとそのマップファイルが記録されている。

【００７６】

再生制御部６５は、読み出し制御部６１に対して、マップファイルを読み出すように指示する。そして、読み出し制御部６１は、記録媒体６０からマップファイルを読み出し、復調部６２、誤り訂正部６３、ファイルシステム部６４の処理を経て、再生制御部６５へマップファイルを入力する。

【００７７】

再生制御部６５は、ＡＶプログラムのＰＭＴのトランスポートパケットのＰＩＤ、プログラムを構成するビデオデータのトランスポートパケットのＰＩＤ、ビデオデータのｓｔｒｅａｍ＿ｔｙｐｅ、プログラムを構成するオーディオデータのトランスポートパケットのＰＩＤ、オーディオデータのｓｔｒｅａｍ＿ｔｙｐｅ、ＰＣＲ＿ＰＩＤを図示しないデマルチプレクサとＡＶデコーダへ供給する。

【００７８】

ユーザーインタフェースによってランダムアクセス再生を指示された場合、再生制御部６５は、内部に記憶されているマップデータの内容に基づいて、記憶媒体６０からのデータの読み出し位置を決定し、ランダムアクセス制御情報を読み出し制御部６１へ入力する。例えば、ユーザーによって選択されたプログラムをある時刻から途中再生をする場合、再生制御部６５は、タイムスタンプのリストから指定された時刻にもっとも近いタイムスタンプを見つけ出し、そのタイムスタンプに対応するトランスポートストリームのアドレスにあるＩピクチャからデータを読み出すように読み出し制御部６１へ指示する。また、ユーザーによって選択されたプログラムを高速再生をする場合、再生制御部６５は、そのプログラムに対応するランダムアクセスポイントのデータに基づいて、プログラムの中のＩピクチャデータを順次連続して読み出すように読み出し制御部６１へ指示する。

【００７９】

読み出し制御部６１は、指定されたランダムアクセスポイントからデータを読み出し、読み出されたデータは、復調部６２、誤り訂正部６３、ファイルシステム部６４の処理を経て、トランスポートストリームを出力する。

【００８０】

次に、ユーザデータが光ディスク１１に記録される場合の暗号化処理部４における処理手順を、図１１のフローチャートを参照して説明する。なお、この例の場合、媒体識別情報DiscIDは、光ディスク１１製造時に、光ディスク１１に書き込まれているものとする。

【００８１】

最初に、ステップＳ１１において、DiscID暗号化復号回路４１は、光ディスク１１のリードインエリアから読み出された、暗号化されている媒体識別情報DiscIDであるＥDiscIDを受け取る。DiscID暗号化復号回路４１は、さらに、ステップＳ１２において、自身が持っているシステム共通秘密に基づいて、ＥDiscIDを復号して、DiscIDを生成し、Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｅに出力する。システム共通秘密は、著作権者から適正なライセンスを受けるときに、与えられたものである。

【００８２】

ステップＳ１３において、Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、Ｋｅｍ発生モジュール４２のＫｍメモリ４２Ａからマスタキー－Ｋｍを読み出す。Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、さらに、ステップＳ１４で、上述の式（１）に従い、光ディスク１１の媒体識別情報DiscIDとマスタキー－Ｋｍの結合にｈａｓｈ関数を適用して、イフェクティブマスタキー－Ｋｅｍを計算し、Ｋｄ暗号化復号回路４４に供給する。

【００８３】

次に、ステップＳ１５において、Ｋｄ暗号化復号回路２６は、光ディスク１１のリードインエリアから読み出された暗号化ディスクキーＥＫｄを受け取る。Ｋｄ暗号化復号回路２６は、ステップＳ３６で、光ディスク１１のリードインエリアに、暗号化ディスクキーＥＫｄが書き込まれているか否か（暗号化ディスクキーＥＫｄを受け取ることができたか否か）の判定を行う。暗号化ディスクキーＥＫｄが書き込まれていないと判定された場合、ステップＳ３７に進み、乱数発生回路４３は、ｄビット、具体的には例えば５６ビットの乱数を発生し、ディスクキー－Ｋｄとして、Ｋｄ暗号化復号回路４４に出力する。

【００８４】

次に、ステップＳ１８において、Ｋｄ暗号化復号回路４４は、乱数発生回路４３から供給されたディスクキー－Ｋｄをハッシュ関数回路４２Ｂから受け取ったイフェクティブマスタキー－Ｋｅｍにより暗号化して、暗号化ディスクキーＥＫｄを生成し、光ディスク１１のリードインエリアに記録する。

【００８５】

ステップＳ１６で、暗号化ディスクキーＥＫｄが書き込まれていると判定された場合、ステップＳ１９に進み、Ｋｄ暗号化復号回路４４は、この光ディスク１１のリードインエリアＡｋｒｅａｄｉｎから読み出された暗号化ディスクキーＥＫｄをハッシュ関数回路４２Ｂから受け取ったイフェクティブマスタキーＫｅｍで復号して、ディスクキーＫｄを得る。Ｋｄ暗号化復号回路４４は、そのディスクキーＫｄを、Ｋｃ暗号化回路４５に出力する。

【００８６】

ステップＳ１８又はＳ１９の処理の後、ステップＳ２０で、Ｋｃ暗号化回路４５は、インタフェース部からコンテンツキーＫｃと暗号化コンテンツデータを受け取り、ステップＳ２１でコンテンツキーＫｃをＫｄ暗号化復号回路４４（暗号化ディスクキーＥＫｄが光ディスク１１に記録されている場合）、又は乱数発生回路４３（暗号化ディスクキーＥＫｄが光ディスク１１に記録されていない場合）から受け取ったディスクキーで暗号化して暗号化コンテンツキーＥＫｃを生成する。Ｋｃ暗号化回路４５は、また、その暗号化コンテンツキーＥＫｃを、光ディスク１１のデータエリアにあるセクタヘッダに記録する。

【００８７】

次に、ステップＳ２２において、コンテンツデータを光ディスク１１のデータエリアのメインデータ部に記録する。

【００８８】

ステップＳ２３において、コンテンツデータ復号回路４６は、インタフェース部から受け取ったコンテンツキーＫｃを用いて暗号化コンテンツデータを復号し、平文のコンテンツデータを生成してマップファイル生成回路４７にわたす。

【００８９】

ステップＳ２４において、マップファイル生成回路４７は、（もしマップファイルがなければあらたに生成し、）平文コンテンツデータから再生時に必要となる情報を抜き出してマップファイルに追加する。

【００９０】

上述のマップファイル生成回路４７のストリーム解析部４７５の動作例を図１

２と図１３のフローチャートを用いて説明する。図１２は、ビデオデータのトランスポートパケットの解析動作を説明するものであり、また、図１３は、オーディオデータのトランスポートパケットの解析動作を説明するものである。

【００９１】

先ず、図１２に示すフローチャートを参照して、ビデオデータのトランスポートパケットの解析動作を説明をする。

【００９２】

ステップＳ３１において、ストリーム解析部４７５は、記録するＡＶプログラムのビデオのＰＩＤとそのｓｔｒｅａｍ＿ｔｙｐｅがＰＡＴ／ＰＭＴ解析部４７４によって入力される。

【００９３】

ステップＳ３２において、ストリーム解析部４７５は、ビデオデータのトランスポートパケットを受信する。ストリーム解析部４７５にはビデオバッファが内蔵されている。ストリーム解析部４７５は、ビデオデータのトランスポートパケットを受信すると、そのペイロードをビデオストリームバッファへ入力する。

【００９４】

ステップＳ３３において、ストリーム解析部４７５は、ビデオストリームバッファの中のストリームにＭＰＥＧビデオのsequence_header_code(32ビット長で"0x000001B3"の符号)が含まれるか否かを調べる。具体的には、バッファ内のストリームの先頭から1バイトずつシフトしてsequence_header_code とマッチングするか否かを調べる。検査の終わったバイトは、ビデオストリームバッファから捨てる。

【００９５】

ステップＳ３３でストリームにsequence_header_codeが含まれていない時は、ステップＳ３２へ戻る。ステップＳ３２が２回目以降である場合は、ビデオパケットのペイロードをビデオバッファの最後のデータへ追加入力(append)する。

【００９６】

ステップＳ３３でストリームにsequence_header_codeが含まれていた時は、ステップＳ３４において、sequence_header_code の第1バイト目を含むトランスポ

ートパケットをランダムアクセスする時のＩピクチャデータの読み出し開始ポイントとする。

【００９７】

ステップＳ３５において、ストリーム解析部４７５は、上記パケットの読み出しの開始ポイントをマップデータ作成部４７７へ知らせる。マップデータ作成部４７７へは、ランダムアクセスポイントのアドレスとして記録するトランスポートストリームの先頭からそのパケットまでのバイト数が、カウンター部４７６から入力され、またランダムアクセスポイントのタイムスタンプとして、そのパケットのペイロードに含まれるＩピクチャのＰＴＳ(Presentation Time Stamp) が入力される。

【００９８】

ステップＳ３６において、ストリーム解析部４７５は、現在のパケットが最後の入力パケットであるかどうかを判定する。最後のパケットでない場合、ステップＳ３２へ戻る。最後のパケットである場合、処理を終了する。

【００９９】

次に、図１３を用いてオーディオデータのトランスポートパケットの解析動作を説明をする。

【０１００】

ステップＳ４１において、ストリーム解析部４７５は、記録するプログラムのオーディオデータのＰＩＤとそのstream_typeがPAT/PMT解析部４７４によって入力される。

【０１０１】

ステップＳ４２において、ストリーム解析部４７５は、オーディオデータのトランスポートパケットを受信する。

【０１０２】

ステップＳ４３において、ストリーム解析部４７５は、ペイロードのオーディオストリームの中にオーディオフレームの第１バイト目のsync_byte が含まれるかを調べる。オーディオフレームは符号化ビットレートにより決まる固定長であるので、この固定長間隔で現れるsync_byte がペイロードに含まれるかどうかを

調べる。

【０１０３】

ステップＳ４３でペイロードにオーディオフレームのsync_byte が含まれていない時は、ステップＳ４２へ戻る。

【０１０４】

ステップＳ４３でペイロードにオーディオフレームのsync_byte が含まれていた時は、ステップＳ４４へ進む。

【０１０５】

ステップＳ４４において、ストリーム解析部４７５は、オーディオフレームのsync_byte を含むパケットをランダムアクセスする時のオーディオフレームの読み出し開始ポイントであることをマップデータ作成部４７７へ知らせる。マップデータ作成部４７７へは、ランダムアクセスポイントのアドレスとして記録するトランスポートストリームの先頭からそのパケットまでのバイト数が、カウンター部４７６から入力され、またランダムアクセスポイントのタイムスタンプとして、そのパケットのペイロードに含まれるオーディオフレームのＰＴＳ(Presentation Time Stamp)が入力される。

【０１０６】

ステップＳ４５において、ストリーム解析部４７５は、現在のパケットが最後の入力パケットであるかどうかを判定する。最後のパケットでない場合、ステップＳ４２へ戻る。最後のパケットである場合、処理を終了する。

【０１０７】

そして、図１１に示したフローチャートのステップＳ２５において、暗号化処理部４の各回路は、すべてのコンテンツデータを記録したか否かの判定を行う。すべてのコンテンツデータがまだ記録されていないと判定された場合、ステップＳ２６に進み、暗号化処理部４の各回路は、光ディスク１１のまだデータを記録していないセクタにアクセスし、ステップＳ２０に戻り、以下同様の処理を繰り返す。ステップＳ４５で、すべてのコンテンツデータが記録されたと判定された場合、暗号化処理部４の各回路は、すべての記録処理を終了する。

【０１０８】

以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のシステム共通秘密で、暗号化されたDiscIDを復号し、媒体識別情報DiscIDを得ることにより、暗号化した情報が記録媒体に記録される。

【０１０９】

次に、製造時に、媒体識別情報DiscIDが記録されていない光ディスク１１に対して、ユーザデータを記録する場合の暗号化処理部４における処理手順を、図１４のフローチャートを参照して説明する。

【０１１０】

最初に、ステップＳ５１において、DiscID暗号化復号回路２１は、光ディスク１１のリードインエリアＡＲreadinから読み出されたＥDiscIDを受け取り、またＫｄ暗号化復号回路４４は、光ディスク１１のリードインエリアＡＲreadinから読み出された暗号化ディスクキーＥＫｄを受け取る。

【０１１１】

次に、ステップＳ５２において、DiscID暗号化復号回路４１は、光ディスク１１のリードインエリアＡＲreadinにＥDiscIDが書き込まれているか否か（ＥDiscIDを受けることができたか否か）の判定を行い、Ｋｄ暗号化復号回路４４は、光ディスク１１のリードインエリアＡＲreadinに暗号化ディスクキーＥＫｄが書き込まれているか否か（暗号化ディスクキーＥＫｄを受け取ることができたか否か）の判定を行う。ＥDiscIDと暗号化ディスクキーＥＫｄが共に書き込まれていないと判定された場合、ステップＳ５３に進み、乱数発生回路４３は、Ｉビット、具体的には例えば１２８ビットの乱数を発生し、媒体識別DiscIDとして、DiscID暗号化復号回路４１に出力する。

【０１１２】

次に、ステップＳ５４において、DiscID暗号化復号回路４１は、乱数発生回路４３から供給された媒体識別情報DiscIDを、自身で持っているシステム共通秘密に基づいて暗号化して、ＥDiscIDを生成し、光ディスク１１のリードインエリアＡＲreadinに記録する。

【０１１３】

次に、ステップＳ５５において、Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、Ｋｅｍ発生モジュール４２のＫｍメモリ４２Ａから、マスタキーＫｍを読み出す。Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、ステップＳ５６で、上述の式（１）に従い、光ディスク１１の媒体識別情報DiscID、及びＫｍメモリ４２Ａから読み出したマスタキーＫｍの結合にｈａｓｈ関数を適用して、イフェクティブマスタキーＫｅｍを計算し、Ｋｄ暗号化復号回路４４に供給する。

【０１１４】

次に、ステップＳ５７において、乱数発生回路４３は、ｄビット、具体的には例えば５６ビットの乱数を発生し、ディスクキーＫｄとして、Ｋｄ暗号化復号回路４４に出力する。Ｋｄ暗号化復号回路４４は、ステップＳ５８において、乱数発生回路４３から供給されたディスクキーＫｄを、ハッシュ関数回路４２Ｂから受け取ったイフェクティブマスタキーＫｅｍにより暗号化して、暗号化ディスクキーＥＫｄを生成し、光ディスク１１のリードインエリアＡＲreadinに記録する。

【０１１５】

ステップＳ５２で、EDiscIDと暗号化ディスクキーＥＫｄが書き込まれていると判定された場合、ステップＳ５９に進み、DiscID暗号化復号回路４１は、この光ディスク１１から読み出されたＥDiscIDを、自身が持っているシステム共通秘密で復号して、媒体識別情報DiscIDを生成する。

【０１１６】

ステップＳ６０において、Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、Ｋｅｍ発生モジュール４２のＫｍメモリ４２Ａから、マスタキーＫｍを読み出す。Ｋｅｍ発生モジュール４２のハッシュ関数回路４２Ｂは、ステップＳ６１で、上述の式（１）に従い、光ディスク１１のDiscIDとマスタキーKmの結合にｈａｓｈ関数を適用して、イフェクティブマスタキーＫｅｍを計算し、Ｋｄ暗号化復号回路４４に供給する。

【０１１７】

次に、ステップＳ６２において、Ｋｄ暗号化復号回路４４は、この光ディスク１１から読み出された暗号化ディスクキーＥＫｄを、ハッシュ関数回路４２Ｂから受け取ったイフェクティブマスタキーＫｅｍで復号して、ディスクキーＫｄを得る。Ｋｄ暗号化復号回路２４４、ディスクキーＫｄをＫｃ暗号化回路４５に出力する。

【０１１８】

ステップＳ５８又はステップＳ６２の処理の後は、ステップＳ６３に進むが、ステップＳ６３乃至ステップＳ７０で行われる処理は、図１１のステップＳ２０乃至ステップＳ２７で行われる処理と同様の処理であり、すべてのコンテンツデータが記録されたと判定された場合、すべての記録処理が終了する。

【０１１９】

以上のようにして、媒体識別情報DiscIDが生成され、記録媒体に記録され、そして生成された媒体識別情報DiscIDとマスタキーＫｍに対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、既存の記録媒体（DiscIDが記録されていない記録媒体）に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【０１２０】

次に、図１５のフローチャートを参照して、復号処理部５により行われるユーザデータの再生処理を説明する。最初に、ステップＳ８１において、ＥDiscID復号回路５１は、光ディスク１１のリードインエリアＡＲreadinから読み出された、暗号化された媒体識別情報DiscIDであるＥDiscIDを受け取る。ＥDiscID復号回路５１はさらに、ステップＳ８２において、自身が持つシステム共通秘密に基づいて、ＥDiscIDを復号して媒体識別情報DiscIDを生成し、Ｋｅｍ発生モジュール５２のハッシュ関数回路５２Ｂに出力する。

【０１２１】

次に、ステップＳ８３において、Ｋｅｍ発生モジュール５２のハッシュ関数回路５２Ｂは、ＥDiscID復号回路５１から出力された媒体識別情報DiscIDを受け取

るとともに、Ｋｍメモリ５２ＡからマスタキーＫｍを読み出し、上述の式（１）に従い、光ディスク１１の媒体識別情報DiscIDとマスタキーＫｍの結合にｈａｓｈ関数を適用してイフェクティブマスタキーＫｅｍを算出し、ＥＫｄ復号回路５４に供給する。

【０１２２】

ステップＳ８４において、ＥＫｄ復号回路５４は、光ディスク１１のリードインエリアＡＲreadinから読み出された暗号化ディスクキーＥＫｄを受け取る。ＥＫｄ復号回路５４は、ステップＳ８５で、この読み出された暗号化ディスクキーＥＫｄを、ハッシュ関数回路５２Ｂから受け取ったイフェクティブマスタキーＫｅｍで復号して、ディスクキーＫｄを算出し、ＥＫｃ復号回路５５に出力する。

【０１２３】

次に、ステップＳ８６において、制御回路１７はマップファイルを光ディスク１１から読み出し、これを用いてコンテンツデータの読み出し場所を決める。

【０１２４】

ステップＳ８７において、ＥＫｃ復号回路５５は、光ディスク１１のデータエリアＡＲdataから読み出された各セクタの暗号化コンテンツキーＥＫｃを受け取る。ＥＫｃ復号回路５５は、ステップＳ８８で、この読み出された暗号化コンテンツキーＥＫｃを、ＥＫｄ復号回路５４から受け取ったディスクキーＫｄで復号して、コンテンツキーＫｃを算出し、ステップＳ８９でインタフェース部にわたす。

【０１２５】

ステップＳ９０で、光ディスク１１のデータエリアＡＲdataから暗号化されたコンテンツデータを読み出してインタフェース部にわたす。

【０１２６】

次に、ステップＳ９１において、復号部５の各回路は、光ディスク１１のデータエリアＡＲdataから、必要なすべてのコンテンツデータを読み出したか否かの判定を行う。すべてのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ９２に進み、復号部５の各回路は、光ディスク１１の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ８６以降の処理

を繰り返す。必要なすべてのコンテンツデータが読み出されたと判定された場合、復号部５の各回路は、すべての再生処理を終了する。

【０１２７】

以上は、図８に示したように、暗号化されたまま読み出されたコンテンツデータと、復号したコンテンツキーKcとを、データインタフェース部に渡すようになっている場合の処理である。

【０１２８】

これは例えば、このコンテンツを他の機器に伝送するような場合に用いられる。

【０１２９】

これに対し、図９に示した復号処理部５のように、コンテンツ復号回路５６において、光ディスク１１のデータエリアＡＲdataから上記記録／再生ヘッド１３により読み出された暗号化コンテンツデータをＥＫｃ復号回路５５で復号したコンテンツキーＫｃにより復号して平文コンテンツデータを生成する場合の処理例を、図１６のフローチャートを用いて説明する。

【０１３０】

これは例えば、この再生機器においてこの後コンテンツに施されているＭＰＥＧなどの符号が復号され、Ｄ／Ａコンバータを通して画像として出力される場合に用いられる。

【０１３１】

図１６に示したフローチャートにおけるステップＳ１０１乃至ステップＳ１０８は、図１５に示したフローチャートにおけるのステップＳ８１乃至ステップＳ８８と同じ処理であるので説明を省略する。

【０１３２】

ステップＳ１０９で、コンテンツ復号回路５６は、光ディスク１１から読み出した、暗号化されているコンテンツデータを、ＥＫｃ復号回路５５からわたされたコンテンツキーＫｃを用いて復号し、平文コンテンツデータを生成してこれを例えばこの光ディスクプレーヤーが持つＭＰＥＧデコーダーなどに出力する。

【０１３３】

ステップＳ１１０において、復号部５の各回路は、光ディスク１１のデータエリアＡＲdataから、必要なすべてのコンテンツデータを読み出したか否かの判定を行う。すべてのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ１１１に進み、復号部５の各回路は、光ディスク１１の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ１０６以降の処理を繰り返す。必要なすべてのコンテンツデータが読み出されたと判定された場合、復号部５の各回路は、すべての再生処理を終了する。

【０１３４】

このように、記録媒体のＩＤを生成し、所定のシステム共通秘密で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできるようにする。

【０１３５】

上記実施例において、コンテンツデータ及び暗号化コンテンツキーＥＫｃを、光ディスクのセクタごとに記録、再生するようにしているが、このセクタは光ディスクの物理セクタに必ずしも一致する必要はなく、幾つかの物理セクタ若しくは論理セクタを合わせたものなどあらかじめ定められた範囲であるとか、記録時ごとに決められる範囲であってもよい。

【０１３６】

また、上記実施の形態において、ディスクキーＫｄは光ディスク一枚につきひとつずつ使用されるようになっているが、これについてもひとつである必要はなく、あらかじめ定められた光ディスクのブロックごとにひとつずつ使用したり、記録時ごとにひとつずつ使用してもよい。

【０１３７】

さらに、上記実施の形態においてマップファイルをコンテンツキーやディスクキーで暗号化して光ディスクに記録してもよい。

【０１３８】

本発明は、光ディスク以外の記録媒体にデータを記録又は再生する場合にも適用が可能である。

【０１３９】

【発明の効果】

以上のように、本発明によれば、記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータを復号して、再生時に必要な情報を集めたマップファイルを作成し、これをコンテンツデータとともに記録するようにすることで、再生時に必要な情報を持たない方法に比べて、きめ細かなトリックプレイを行える。

【図面の簡単な説明】

【図１】

本発明を適用した光ディスク記録／再生装置の構成を示すブロック図である。

【図２】

上記光ディスクに記録されたデータの構造を模式的に示す図である。

【図３】

上記光ディスク記録／再生装置における暗号化処理部の具体的な構成を示すブロック図である。

【図４】

上記暗号化処理部のマップファイル生成回路の具体的な構成例を示すブロック図である。

【図５】

上記マップファイル生成回路のＰＡＴ／ＰＭＴ解析部の動作を示すフローチャートである。

【図６】

ＭＰＥＧ方式におけるビデオデータのランダムアクセスポイントリストの概念図である。

【図７】

トランスポートストリームとマップファイルの説明図である。

【図８】

上記光ディスク記録／再生装置における復号処理部の具体的な構成例を示すブ

ロック図である。

【図９】

上記復号処理部の他の構成例を示すブロック図である。

【図１０】

マップファイルに含まれる情報を用いてコンテンツデータの読み出しを制御するコンテンツデータ再生装置の構成を示すブロック図である。

【図１１】

ユーザデータが光ディスクに記録される場合の暗号化処理部における処理手順示すフローチャートである。

【図１２】

上記マップファイル生成回路のストリーム解析部によるビデオデータのトランスポートパケットの解析動作を示すフローチャートである。

【図１３】

上記ストリーム解析部によるオーディオデータのトランスポートパケットの解析動作を示すフローチャートである。

【図１４】

製造時に、媒体識別情報DiscIDが記録されていない光ディスクに対して、ユーザデータを記録する場合の暗号化処理部における処理手順を示すフローチャートである。

【図１５】

上記復号処理部により行われるユーザデータの再生処理を示すフローチャートである。

【図１６】

上記復号処理部により行われるユーザデータの再生処理を示すフローチャートである。

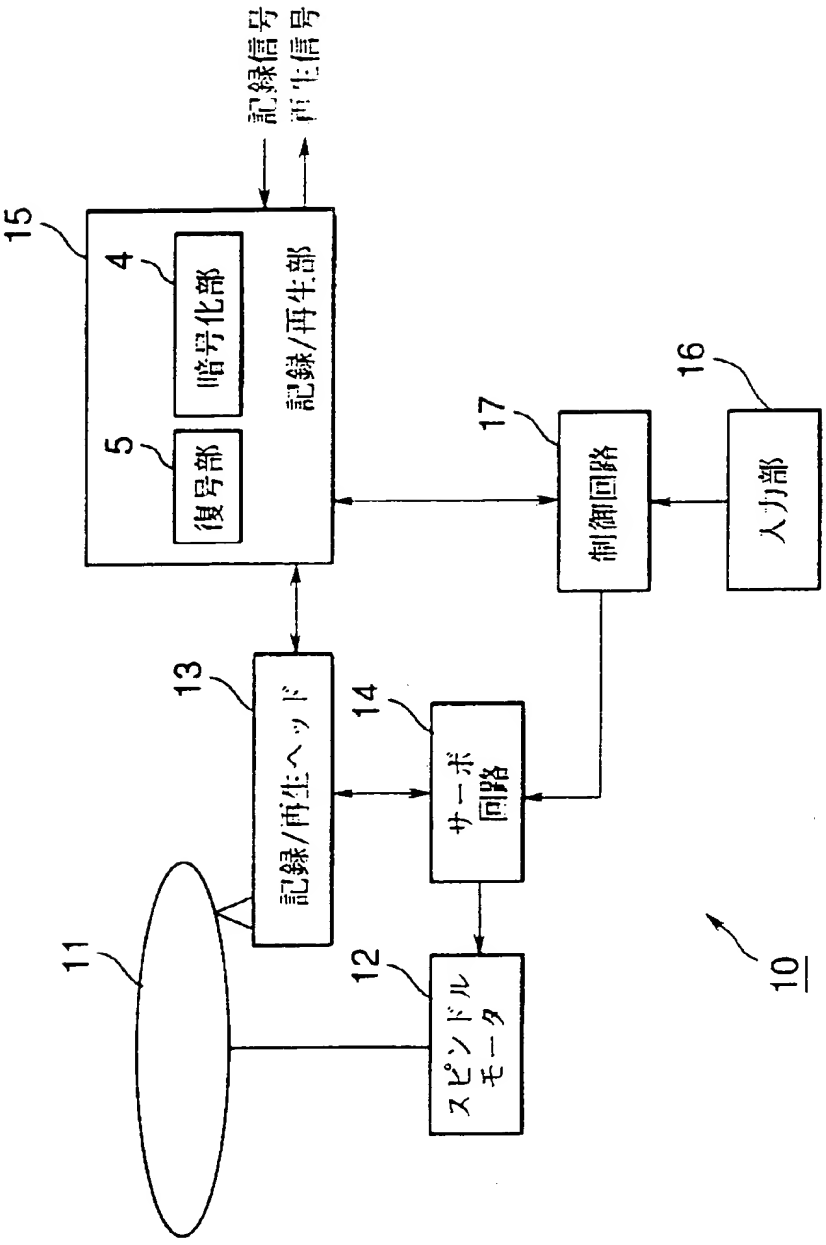
【符号の説明】

４　暗号化処理部、５　復号処理部、１０　光ディスク記録／再生装置、１１　光ディスク、１２　スピンドルモータ、１３　記録／再生ヘッド、１４　サーボ回路、１５　記録／再生部、１６　入力操作部、１７　制御回路、４１　Disc

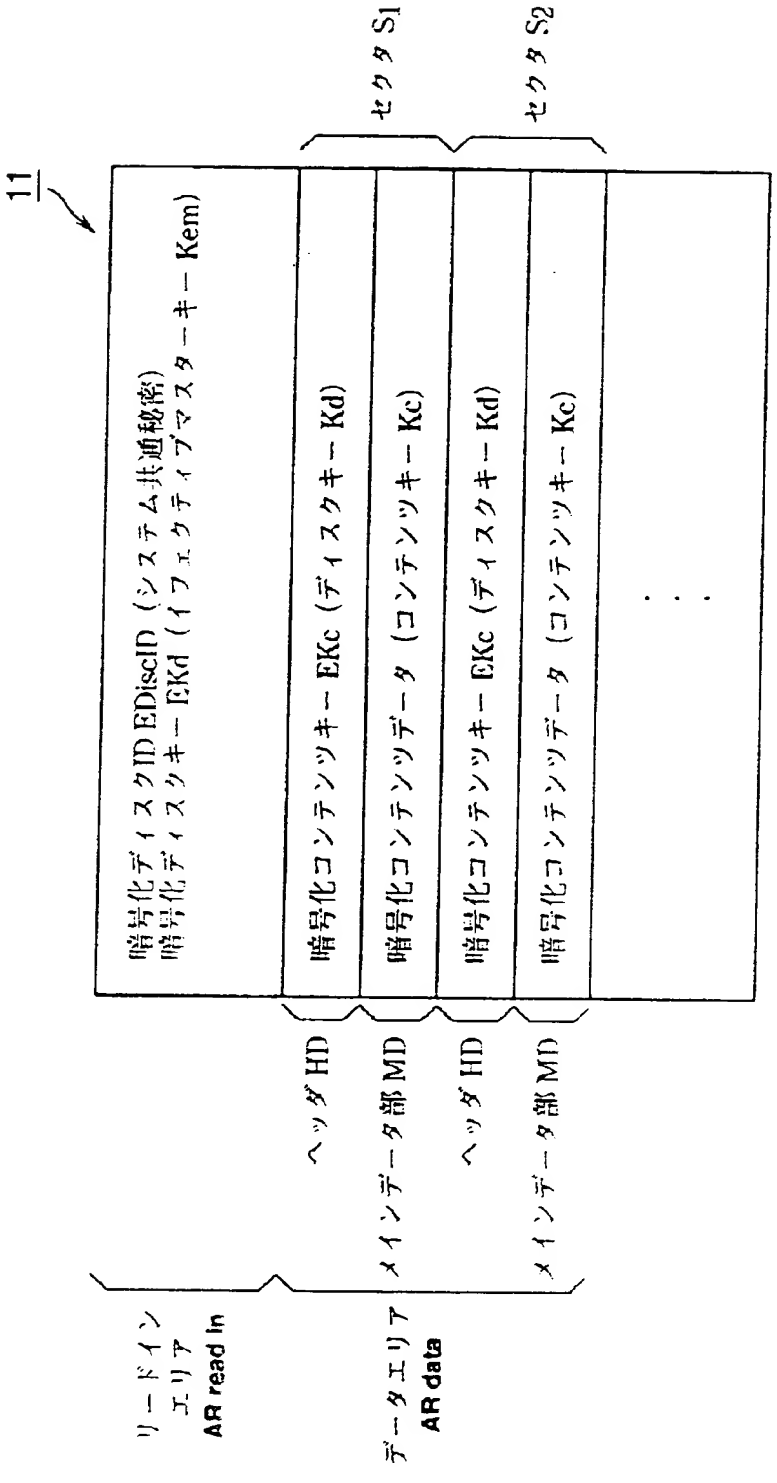
ID暗号化復号回路、４２　Ｋｅｍ発生モジュール、４３　乱数発生回路、４４　Ｋｄ暗号化／復号回路、４５　Ｋｃ暗号化回路、４６　コンテンツデータ復号回路、４７　マップファイル生成回路４７、５１　EDiscID復号回路、５２　Ｋｅｍ発生モジュール、５４　Ｋｄ復号回路、５５　Ｋｃ復号回路、５６　コンテンツ復号回路

【書類名】　図面

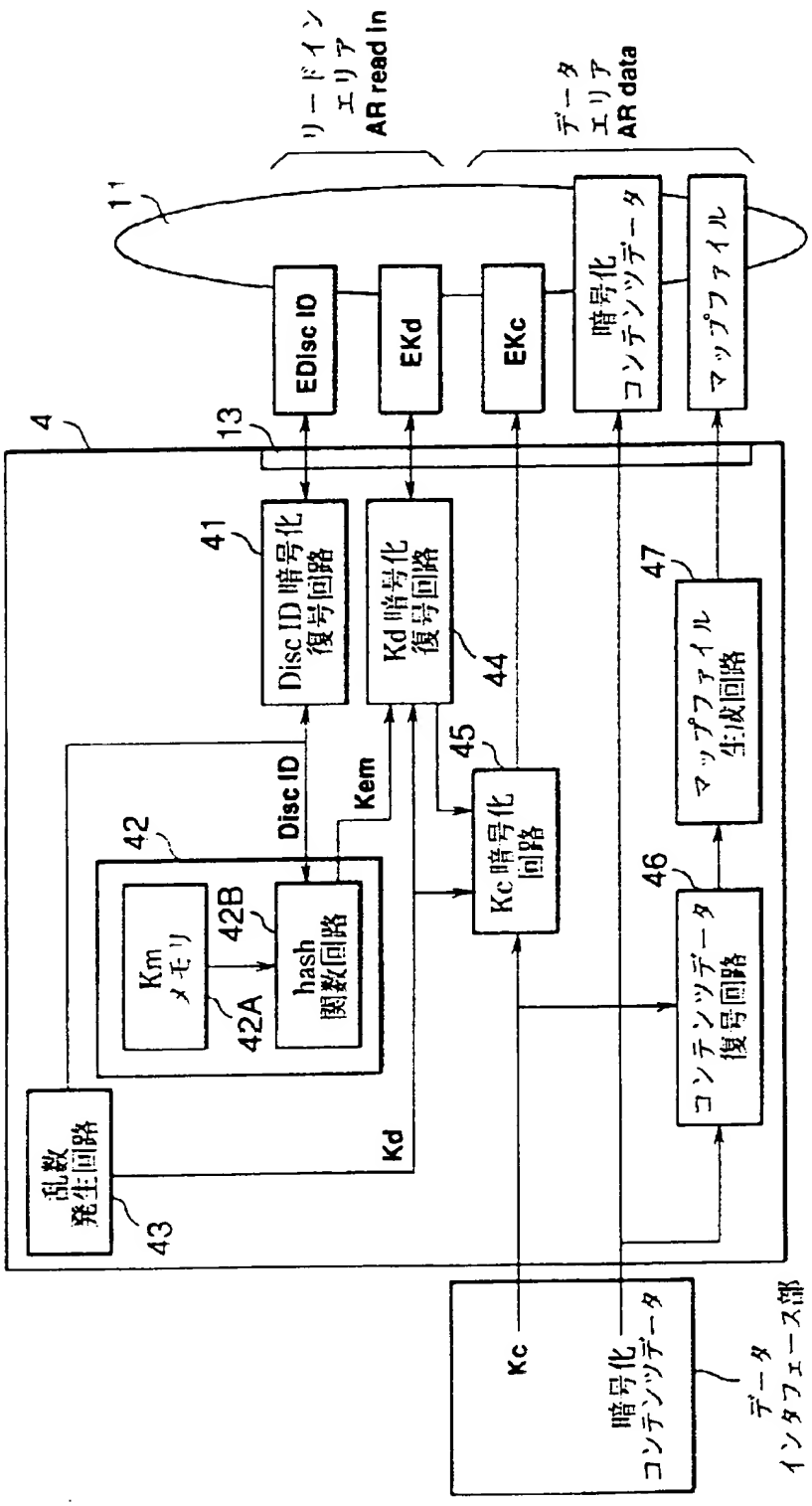
【図１】


記録信号
再生信号
15
4
暗号化部
5
復号部
記録/再生部
17
制御回路
16
入力部
13
記録/再生ヘッド
14
サーボ回路
11
12
スピンドルモータ
10

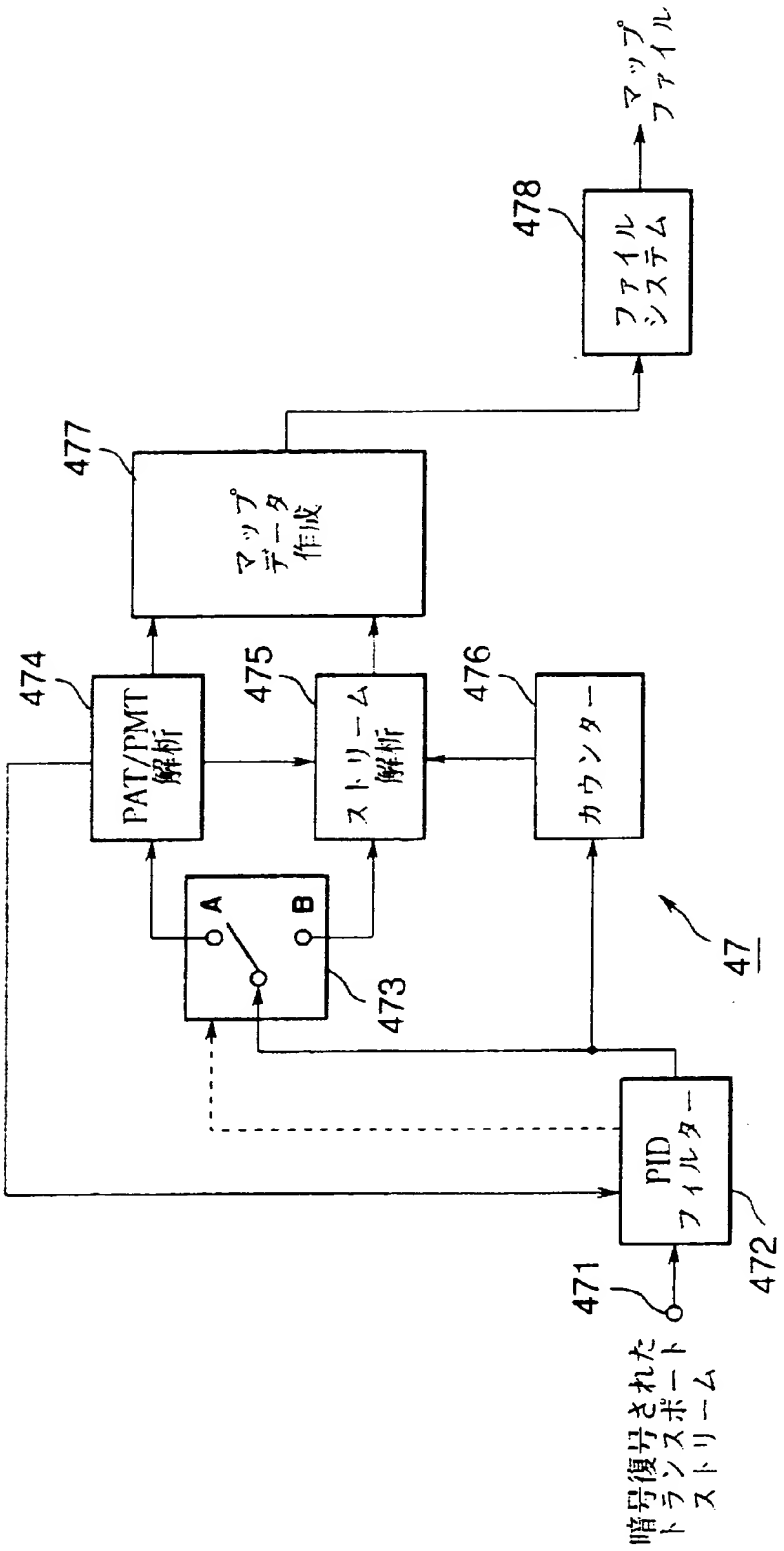
【図２】


11
セクタ S1
セクタ S2
暗号化ディスクID EDiscID（システム共通秘密）
暗号化ディスクキー EKd（イフェクティブマスターキー Kem）
暗号化コンテンツキー EKc（ディスクキー Kd）
暗号化コンテンツデータ（コンテンツキー Kc）
暗号化コンテンツキー EKc（ディスクキー Kd）
暗号化コンテンツデータ（コンテンツキー Kc）
ヘッダ HD
メインデータ部 MD
ヘッダ HD
メインデータ部 MD
リードインエリア AR read in
データエリア AR data

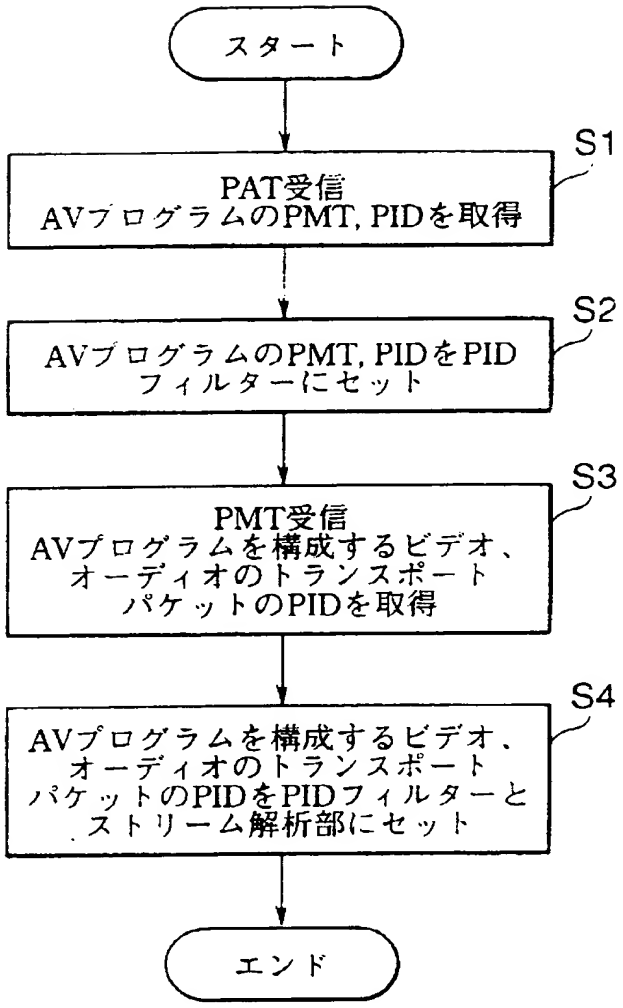
【図３】


リードイン エリア AR read In
データ エリア AR data
11
EDisc ID
EKd
EKc
暗号化 コンテンツデータ
マップファイル
4
13
41
Disc ID 暗号回路 復号回路
Kd 暗号化 復号回路
44
47
マップファイル 生成回路
45
Kem
Disc ID
42
Km メモリ
42B
hash 関数回路
42A
Kc 暗号化 回路
46
コンテンツデータ 復号回路
乱数 発生回路
43
Kd
Kc
暗号化 コンテンツデータ
データ インタフェース部

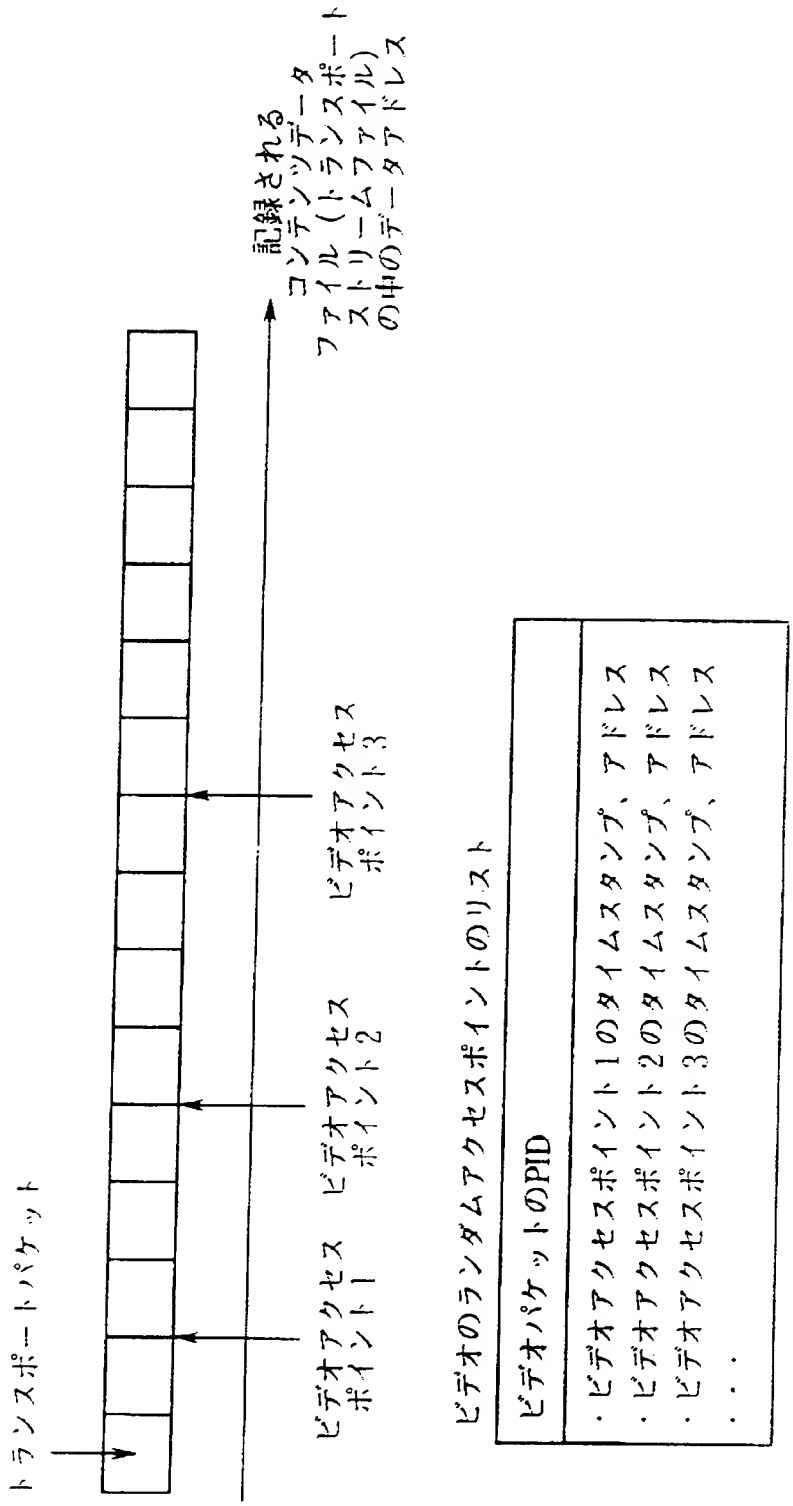
【図４】


暗号復号されたトランスポートストリーム
471
PID フィルター
472
PAT/PMT 解析
474
ストリーム 解析
475
カウンター
476
A
B
473
47
マップ データ 作成
477
ファイル システム
478
マップ ファイル

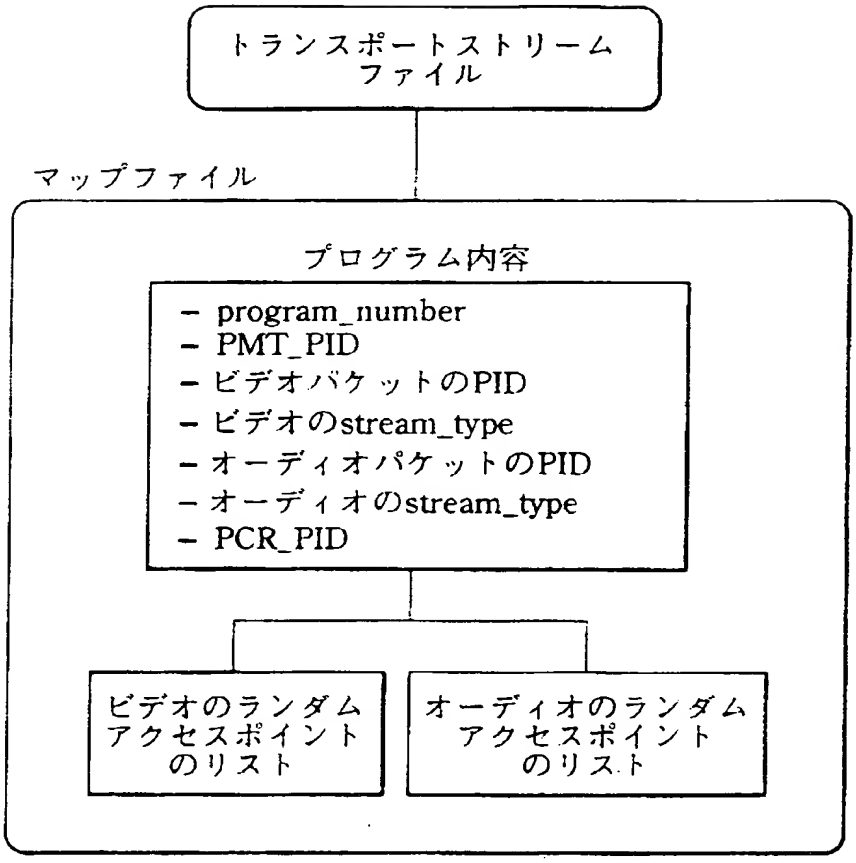
【図５】


スタート
S1
PAT受信
AVプログラムのPMT, PIDを取得
S2
AVプログラムのPMT, PIDをPID
フィルターにセット
S3
PMT受信
AVプログラムを構成するビデオ、
オーディオのトランスポート
パケットのPIDを取得
S4
AVプログラムを構成するビデオ、
オーディオのトランスポート
パケットのPIDをPIDフィルターと
ストリーム解析部にセット
エンド

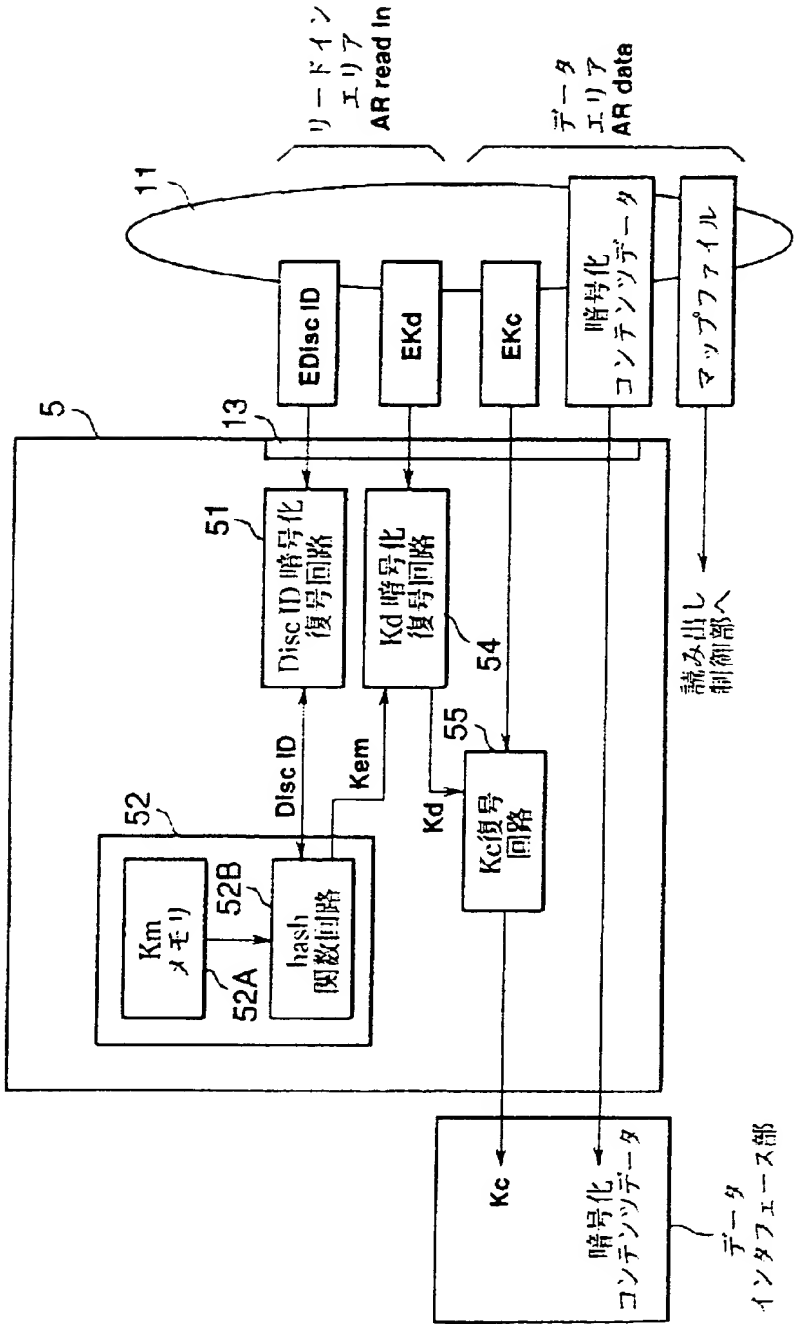
【図６】


トランスポートパケット
ビデオアクセス
ポイント1
ビデオアクセス
ポイント2
ビデオアクセス
ポイント3
記録されるコンテンツデータファイル（トランスポートストリームファイル）の中のデータアドレス
ビデオのランダムアクセスポイントのリスト
ビデオパケットのPID
・ビデオアクセスポイント1のタイムスタンプ、アドレス
・ビデオアクセスポイント2のタイムスタンプ、アドレス
・ビデオアクセスポイント3のタイムスタンプ、アドレス
・・・

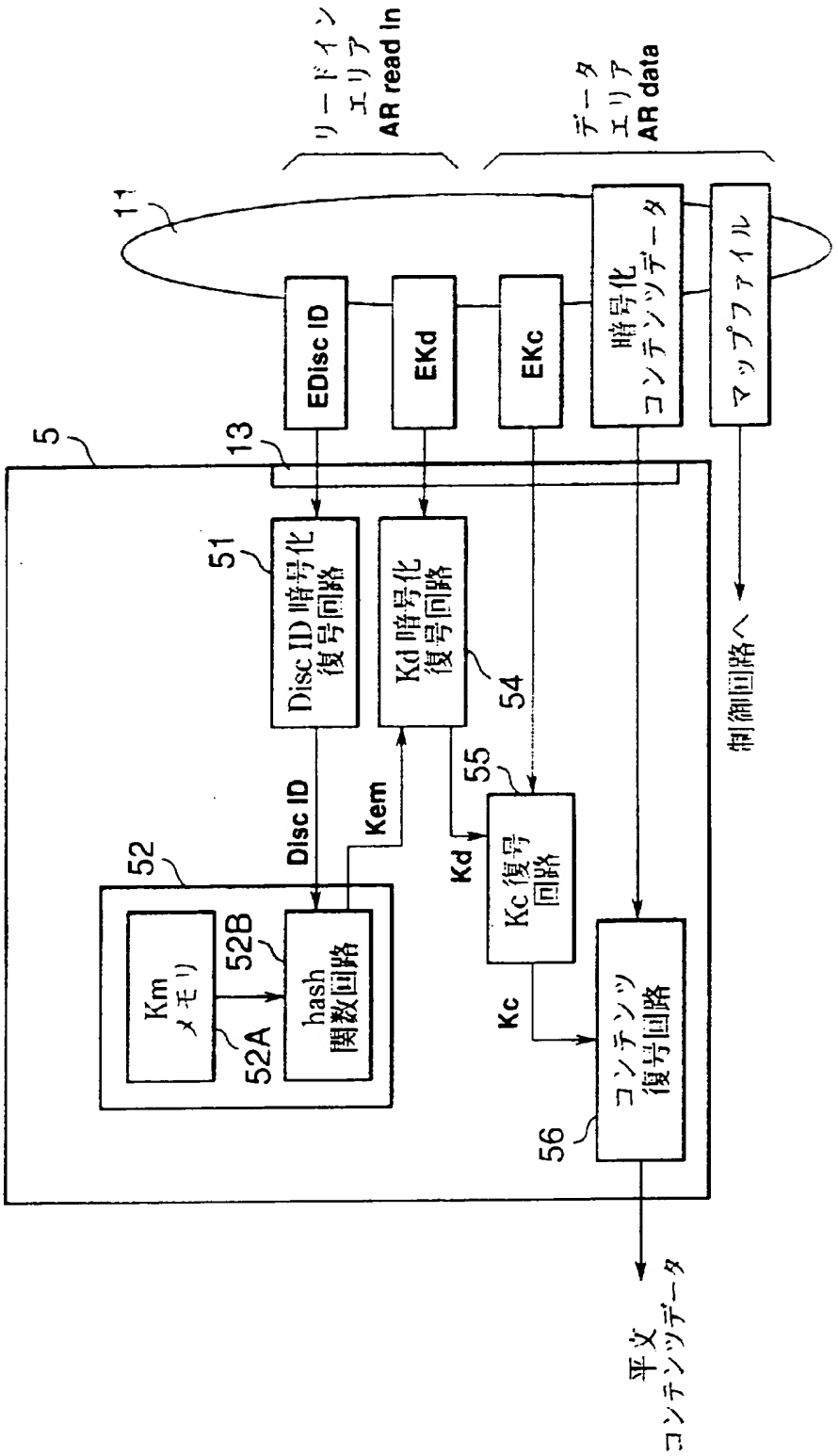
【図７】


トランスポートストリーム
ファイル
マップファイル
プログラム内容
– program_number
– PMT_PID
– ビデオパケットのPID
– ビデオのstream_type
– オーディオパケットのPID
– オーディオのstream_type
– PCR_PID
ビデオのランダム
アクセスポイント
のリスト
オーディオのランダム
アクセスポイント
のリスト

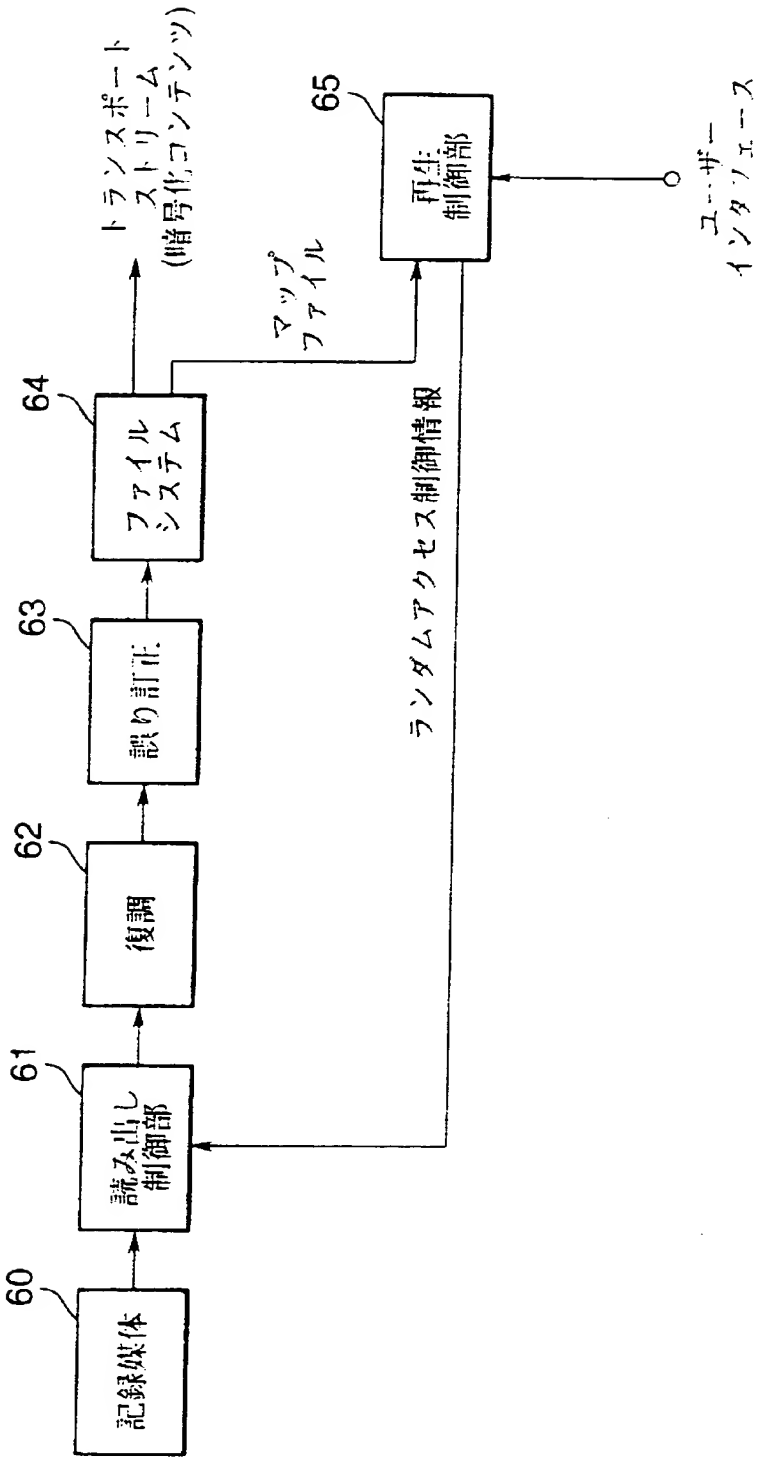
【図８】


リードイン
エリア
AR read In
データ
エリア
AR data
11
EDisc ID
EKd
EKc
暗号化
コンテンツデータ
マップファイル
5
13
51
Disc ID 暗号化
復号回路
Kd 暗号化
復号回路
54
読み出し
制御部へ
55
Disc ID
Kem
Kd
52
Km
メモリ
52B
hash
関数回路
52A
Kc復号
回路
Kc
暗号化
コンテンツデータ
データ
インタフェース部

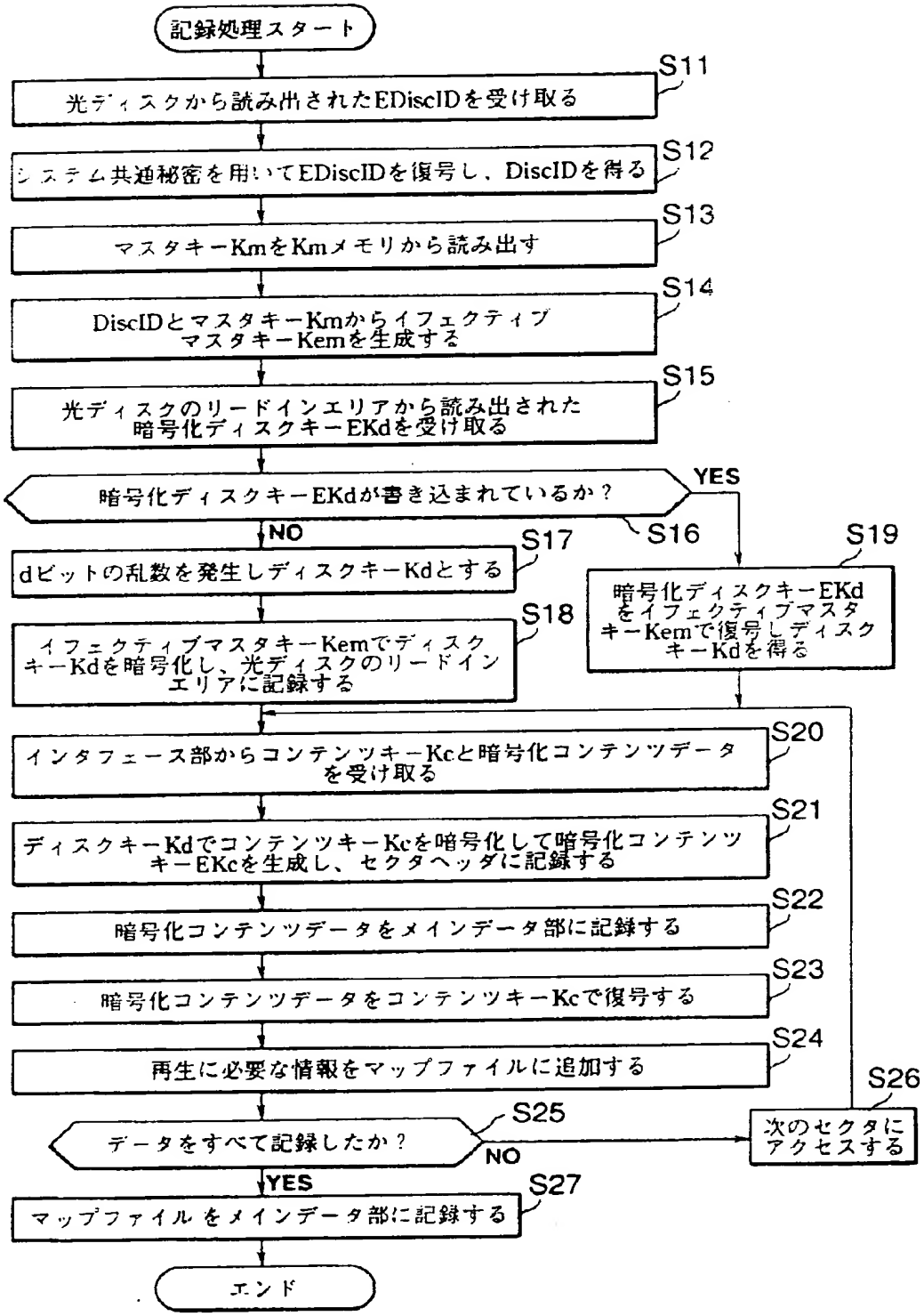
【図９】


リードイン
エリア
AR read In
データ
エリア
AR data
11
EDisc ID
EKd
EKc
暗号化
コンテンツデータ
マップファイル
5
13
51
Disc ID 暗号回路
復号回路
Kd 暗号化
復号回路
54
制御回路へ
55
Disc ID
Kem
52
Km
メモリ
52B
hash
関数回路
52A
Kd
Kc 復号
回路
Kc
コンテンツ
復号回路
56
平文
コンテンツデータ

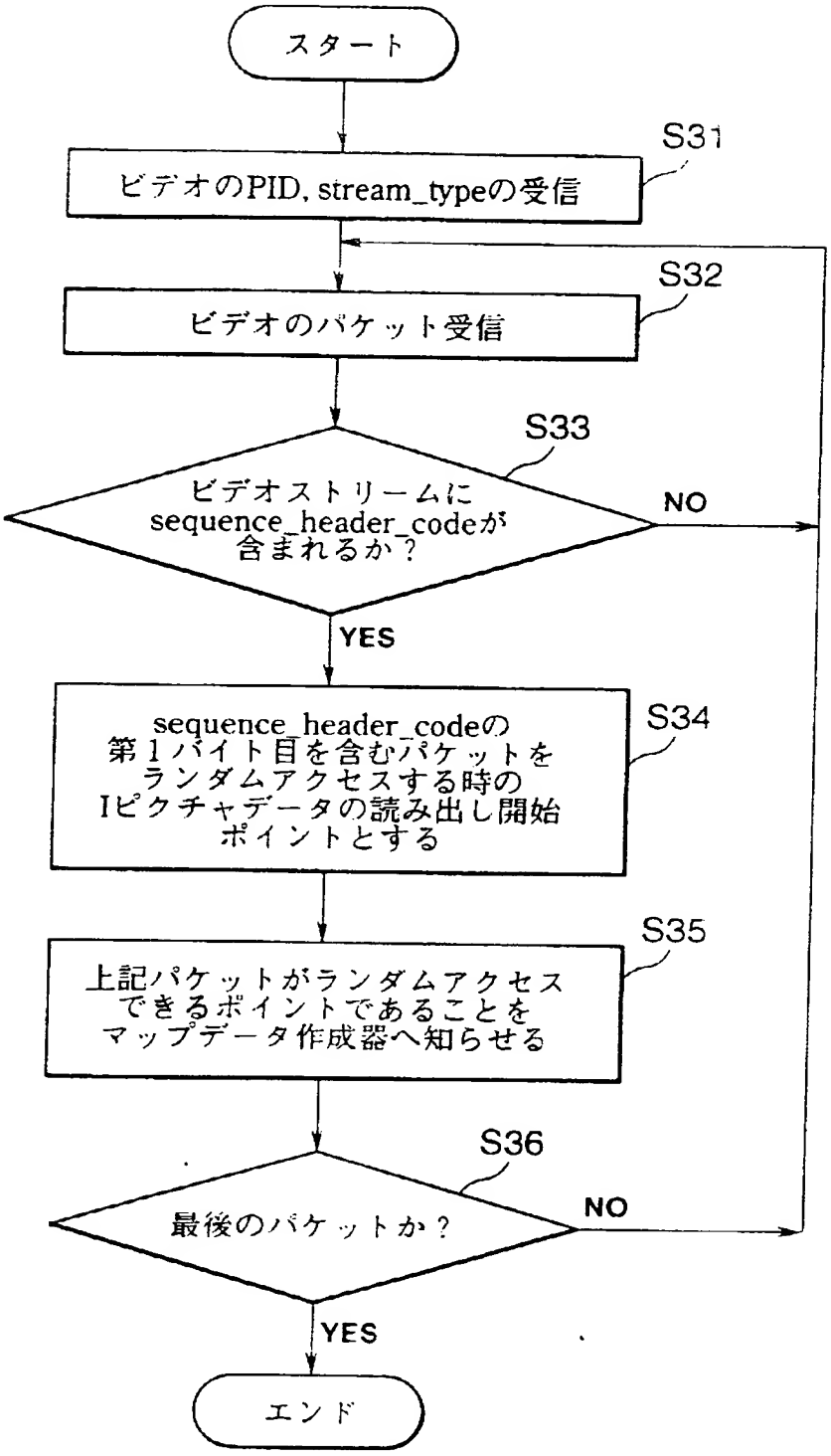
【図１０】


60
記録媒体
61
読み出し制御部
62
復調
63
誤り訂正
64
ファイルシステム
65
再生制御部
トランスポートストリーム
(暗号化コンテンツ)
マップファイル
ランダムアクセス制御情報
ユーザーインタフェース

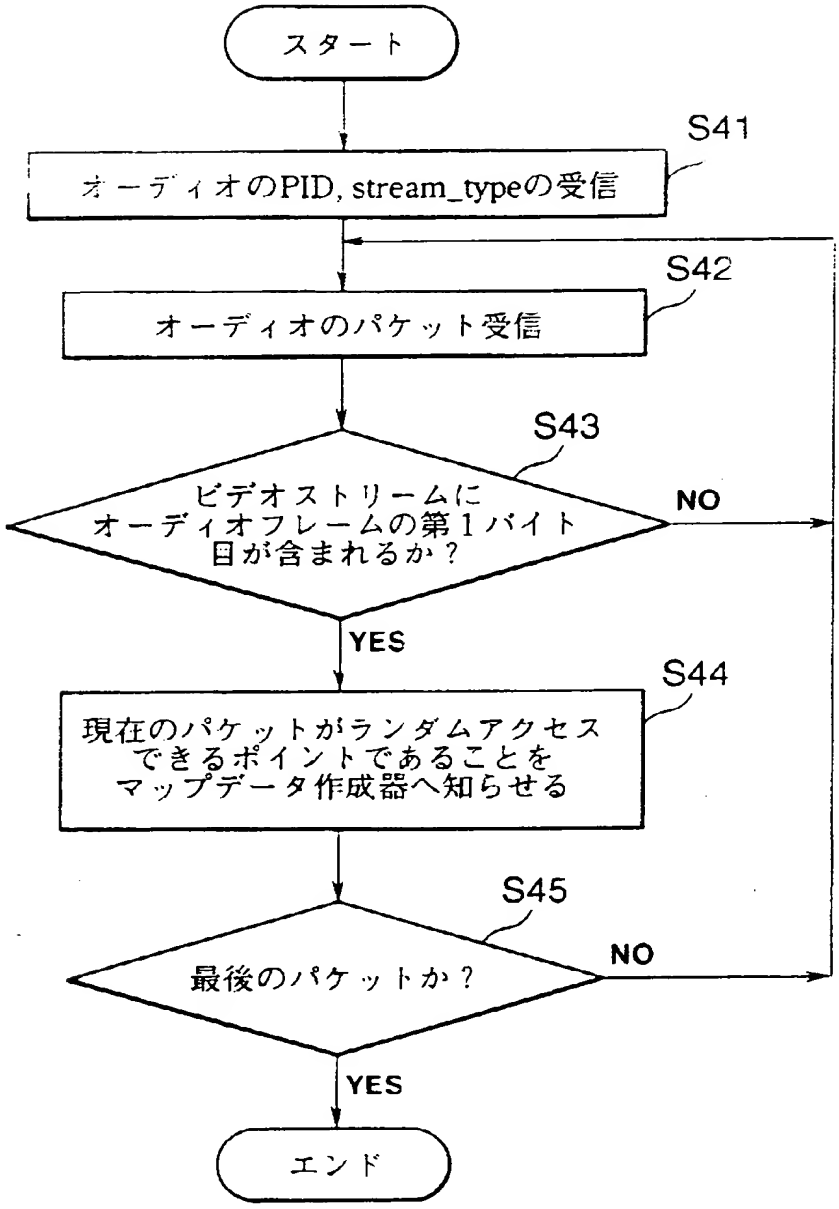
【図１１】


記録処理スタート
S11
光ディスクから読み出されたEDiscIDを受け取る
S12
システム共通秘密を用いてEDiscIDを復号し、DiscIDを得る
S13
マスタキーKmをKmメモリから読み出す
S14
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S15
光ディスクのリードインエリアから読み出された暗号化ディスクキーEKdを受け取る
暗号化ディスクキーEKdが書き込まれているか？
YES
S16
NO
S17
dビットの乱数を発生しディスクキーKdとする
S18
イフェクティブマスタキーKemでディスクキーKdを暗号化し、光ディスクのリードインエリアに記録する
S19
暗号化ディスクキーEKdをイフェクティブマスタキーKemで復号しディスクキーKdを得る
S20
インタフェース部からコンテンツキーKcと暗号化コンテンツデータを受け取る
S21
ディスクキーKdでコンテンツキーKcを暗号化して暗号化コンテンツキーEKcを生成し、セクタヘッダに記録する
S22
暗号化コンテンツデータをメインデータ部に記録する
S23
暗号化コンテンツデータをコンテンツキーKcで復号する
S24
再生に必要な情報をマップファイルに追加する
S26
S25
データをすべて記録したか？
NO
次のセクタにアクセスする
YES
S27
マップファイルをメインデータ部に記録する
エンド

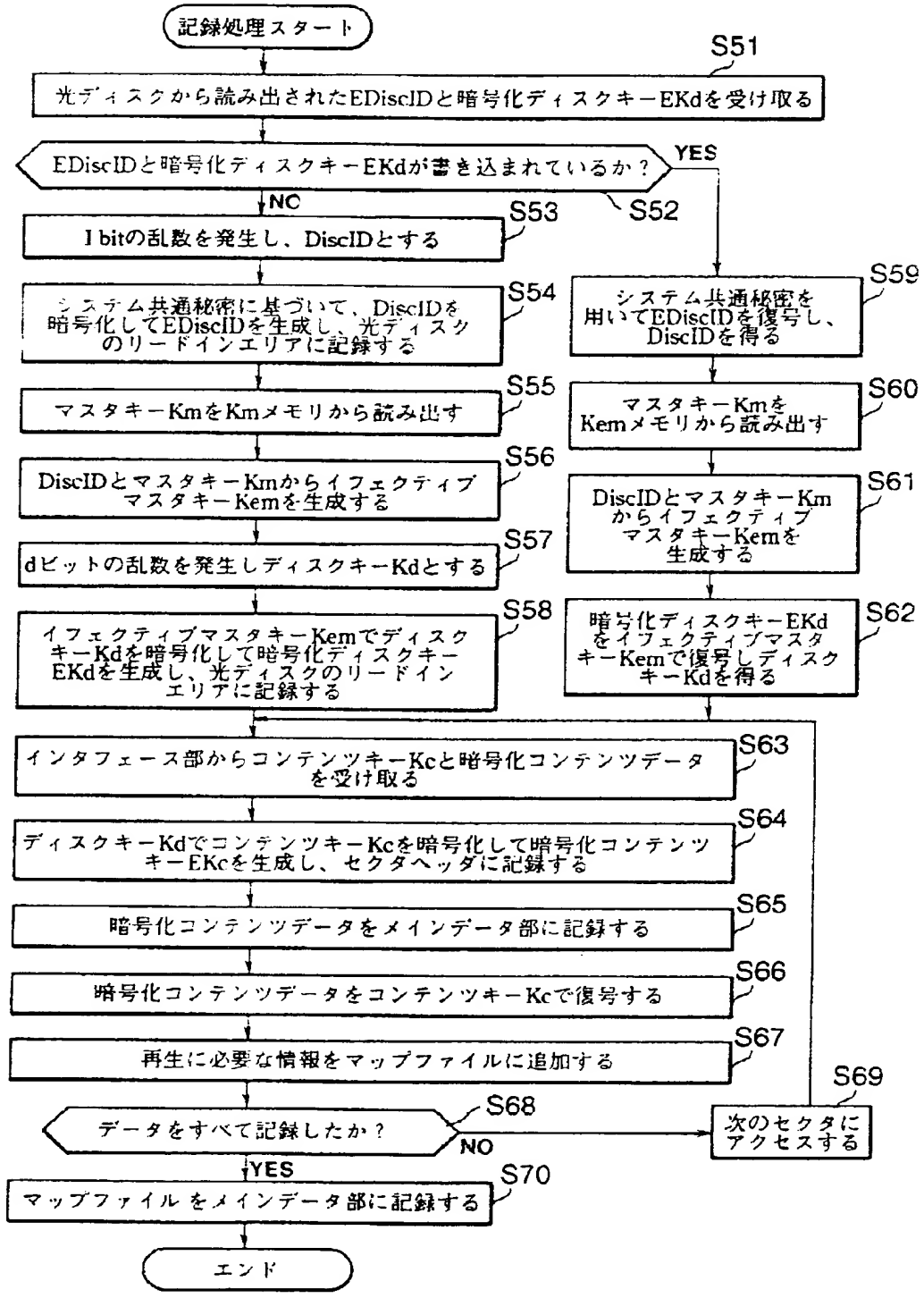
【図１２】


スタート
S31
ビデオのPID, stream_typeの受信
S32
ビデオのパケット受信
S33
ビデオストリームに
sequence_header_codeが
含まれるか？
NO
YES
sequence_header_codeの
第１バイト目を含むパケットを
ランダムアクセスする時の
Iピクチャデータの読み出し開始
ポイントとする
S34
S35
上記パケットがランダムアクセス
できるポイントであることを
マップデータ作成器へ知らせる
S36
最後のパケットか？
NO
YES
エンド

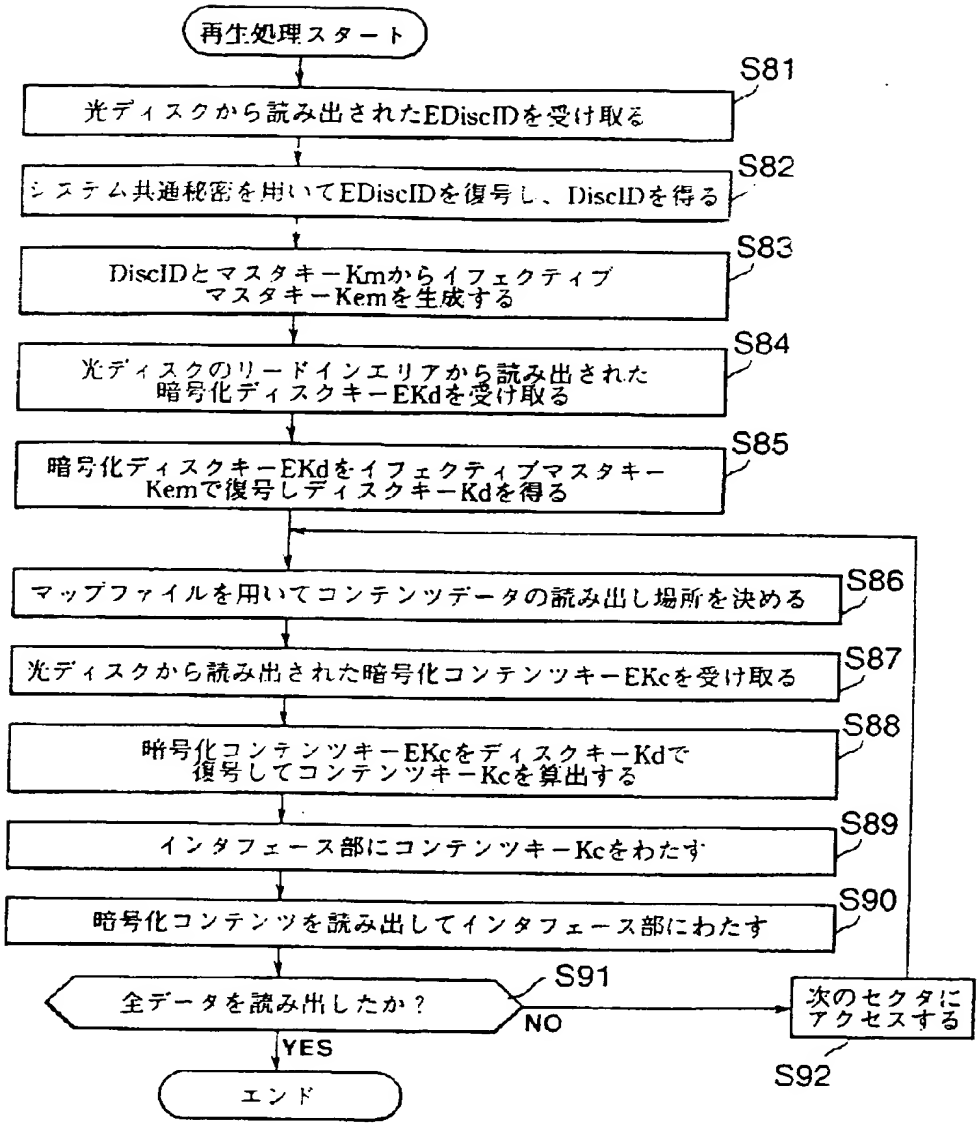
【図１３】


スタート
S41
オーディオのPID, stream_typeの受信
S42
オーディオのパケット受信
S43
ビデオストリームに
オーディオフレームの第１バイト
目が含まれるか？
NO
YES
S44
現在のパケットがランダムアクセス
できるポイントであることを
マップデータ作成器へ知らせる
S45
最後のパケットか？
NO
YES
エンド

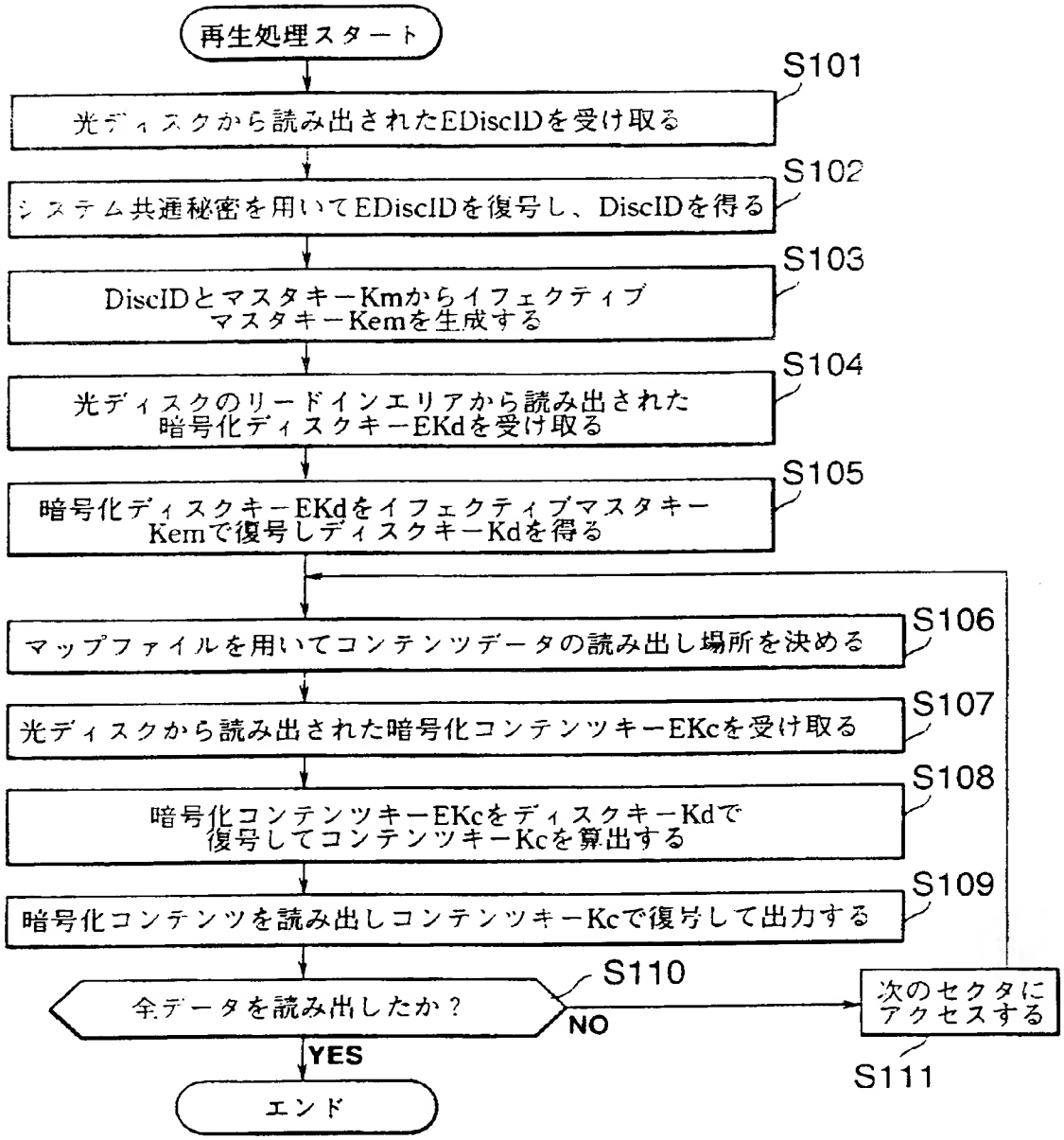
【図１４】


記録処理スタート
S51
光ディスクから読み出されたEDiscIDと暗号化ディスクキーEKdを受け取る
EDiscIDと暗号化ディスクキーEKdが書き込まれているか？
YES
S52
NO
S53
1bitの乱数を発生し、DiscIDとする
S54
システム共通秘密に基づいて、DiscIDを暗号化してEDiscIDを生成し、光ディスクのリードインエリアに記録する
S55
マスタキーKmをKmメモリから読み出す
S56
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S57
dビットの乱数を発生しディスクキーKdとする
S58
イフェクティブマスタキーKemでディスクキーKdを暗号化して暗号化ディスクキーEKdを生成し、光ディスクのリードインエリアに記録する
S59
システム共通秘密を用いてEDiscIDを復号し、DiscIDを得る
S60
マスタキーKmをKemメモリから読み出す
S61
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S62
暗号化ディスクキーEKdをイフェクティブマスタキーKemで復号しディスクキーKdを得る
S63
インタフェース部からコンテンツキーKcと暗号化コンテンツデータを受け取る
S64
ディスクキーKdでコンテンツキーKcを暗号化して暗号化コンテンツキーEKcを生成し、セクタヘッダに記録する
S65
暗号化コンテンツデータをメインデータ部に記録する
S66
暗号化コンテンツデータをコンテンツキーKcで復号する
S67
再生に必要な情報をマップファイルに追加する
S68
データをすべて記録したか？
NO
S69
次のセクタにアクセスする
YES
S70
マップファイルをメインデータ部に記録する
エンド

【図１５】


再生処理スタート
S81
光ディスクから読み出されたEDiscIDを受け取る
S82
システム共通秘密を用いてEDiscIDを復号し、DiscIDを得る
S83
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S84
光ディスクのリードインエリアから読み出された暗号化ディスクキーEKdを受け取る
S85
暗号化ディスクキーEKdをイフェクティブマスタキーKemで復号しディスクキーKdを得る
S86
マップファイルを用いてコンテンツデータの読み出し場所を決める
S87
光ディスクから読み出された暗号化コンテンツキーEKcを受け取る
S88
暗号化コンテンツキーEKcをディスクキーKdで復号してコンテンツキーKcを算出する
S89
インタフェース部にコンテンツキーKcをわたす
S90
暗号化コンテンツを読み出してインタフェース部にわたす
S91
全データを読み出したか？
NO
YES
次のセクタにアクセスする
S92
エンド

【図１６】


再生処理スタート
S101
光ディスクから読み出されたEDiscIDを受け取る
S102
システム共通秘密を用いてEDiscIDを復号し、DiscIDを得る
S103
DiscIDとマスタキーKmからイフェクティブマスタキーKemを生成する
S104
光ディスクのリードインエリアから読み出された暗号化ディスクキーEKdを受け取る
S105
暗号化ディスクキーEKdをイフェクティブマスタキーKemで復号しディスクキーKdを得る
S106
マップファイルを用いてコンテンツデータの読み出し場所を決める
S107
光ディスクから読み出された暗号化コンテンツキーEKcを受け取る
S108
暗号化コンテンツキーEKcをディスクキーKdで復号してコンテンツキーKcを算出する
S109
暗号化コンテンツを読み出しコンテンツキーKcで復号して出力する
S110
全データを読み出したか？
NO
次のセクタにアクセスする
S111
YES
エンド

【書類名】　　要約書

【要約】

【課題】　暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録し、しかも、きめ細かなトリックプレイを行うことができるようにする。

【解決手段】

記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータ復号回路４６によりコンテンツデータを復号して、再生時に必要な管理情報を集めたマップファイルをマップファイル生成回路４７を作成し、これをコンテンツデータとともに記録する。

【選択図】　　図３

出証特２０００－３０４９９７６

出　願　人　履　歴　情　報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社